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

Report on the thematic review of risk management practices related to the operational and remote booking risks of trading activities and data risks

30 March 2023

Contents

A. Introduction

1. The Securities and Futures Commission (SFC) considers sound risk management key to sustaining the resilience of licensed corporations (LCs) amid market uncertainty and volatility.

2. To provide further guidance for LCs to cope with evolving risks, the SFC conducted a thematic review to assess the risk governance and oversight framework of selected LCs, as well as their risk management practices in the following areas.

   (i) **Operational risk management for trading activities** – Operational risk refers to the risk of losses resulting from inadequate or failed internal processes, people and systems. The thematic review in this area focused on the operational risks related to trading activities, covering the management oversight, controls and monitoring implemented by LCs.

   (ii) **Remote booking risk management for trading activities** – Remote booking refers to a business model where an LC, as a trade originating or executing entity, transfers the trading risks (eg, market or credit risk) to an offshore risk-booking affiliate through a group-wide remote booking arrangement. This arrangement may include a transfer pricing arrangement where cost-sharing or profit or loss allocation takes place amongst the group affiliates. The thematic review in this area covered the remote booking and transfer pricing arrangements adopted by LCs and the associated controls and monitoring implemented to address the underlying risks.

   (iii) **Data risk management** – Data risk refers to the risk of operational disruptions and reputational or financial losses due to LCs' deficiencies in managing the data lifecycle, which includes the collection, classification, usage, retention, transfer and disposal of data. The thematic review in this area covered management oversight, controls and monitoring for mitigating the risks at each stage of the data lifecycle, particularly from a data protection perspective.

3. The thematic review commenced with information collection from 48 LCs or financial groups[1] (collectively referred to as the "Groups") through a questionnaire. At a later stage, in-depth discussions and on-site inspections were conducted to review the Groups' management oversight, controls and monitoring in the above risk areas.

4. This report summarises the industry practices in risk governance, oversight and management in each of the three risk areas, together with examples of good practices and areas for improvement observed from the thematic review and other supervisory activities. The SFC's expected standards for LCs to mitigate these specific risks are also set out in this report.

5. The SFC will keep abreast of local and global developments in operational, remote booking and data risk management practices and provide additional guidance to the industry when necessary.

[1] More than one LC may represent a financial group.

B. Operational risk management for trading activities

Background

6. In the context of the review, operational risk refers to the risk of losses resulting from inadequate or failed internal processes, people and systems. While LCs face operational risks in all of their business activities, the thematic review focused on the operational risks arising from trading activities conducted by LCs. The survey results showed that, a majority of the Groups identified "trade related errors and failures" (eg, incorrect order entry and inadvertent breaches of trading or position limits) as the top area of common operational risks[2] in terms of severity (eg, frequency and financial impact).

7. In recent years, operational risk incidents arising from the trading activities of LCs have caused significant losses to firms and their clients and, in some cases, affected market operations. A robust risk governance and control framework is critical for LCs to adequately manage operational risks in their trading activities.

I. Operational risk governance

8. Risk governance refers to an organisational arrangement with defined responsibilities and accountability which enables an LC to properly establish and implement measures to identify, assess, mitigate and report risks.

9. Inadequate operational risk governance may lead to the following issues, which in turn may prevent an LC from effectively identifying and mitigating operational risks:

   - ambiguity as to the roles and responsibilities across functions, which could lower the LCs' effectiveness in addressing operational risk incidents and deterring excessive risk-taking; and

[2] In response to the questionnaire, the Groups were allowed to report one or more areas of operational risk where relevant.

- failure to regularly review the effectiveness of the risk management framework, which could further expose an LC to operational loopholes or emerging types of operational risks.

Expected standards
To address operational risks associated with trading activities, LCs should have in place a sound risk governance framework[3] which should cover the following areas, amongst others: (a) clear definition of the roles, responsibilities and accountability[4] of senior management and relevant functions, to ensure proper implementation of the operational risk management framework (including escalation protocols) and foster a sound risk culture within the LC; and (b) a mechanism to regularly review the adequacy and effectiveness of the operational risk management framework with respect to the LCs' business nature, size, complexity of operations and risk profile.

Market practices

(a) Roles and responsibilities for operational risk management

Responsibilities and accountability of senior management

10. In general, the Groups implemented operational risk governance frameworks and assigned specific roles and responsibilities to their senior management for governing operational risk management.

11. Apart from the Manager-In-Charge (MIC) of Risk Management function, most Groups also designated MICs of other functions (eg, Operational Control and Review, Key Business Lines or both) to oversee the implementation and regular review of operational risk management policies and procedures, including the processes for handling operational risk incidents.

12. Some Groups set up risk governance committees or forums (comprising MICs and other senior management) that convened regular meetings to review the trends and remediation status of operational risk incidents and to assess whether their current risk exposure level remains acceptable.

13. Some Groups defined their operational risk appetite (ie, the level of operational risk a firm is willing to accept) in both quantitative (eg, risk limits and amount of loss) and qualitative (eg, intolerance of certain types of risks and behaviour) terms, taking into consideration their capital and risk profile. These Groups also set out risk strategies (ie,

[3] 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).

[4] Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management issued by the SFC on 16 December 2016.

the direction and focus of how risk management policies would be established and implemented) to address operational risks and align with their risk appetite.

Roles and responsibilities of relevant functions at the operational level

14. A majority of the Groups designated operational risk management roles to different functions by adopting a "three lines of defence" approach.

    (i) The first line of defence refers to frontline staff conducting trading activities and taking up risks (ie, trading unit). Some Groups relied on the supervisors of trading activities (eg, head of trading), while others assigned a specific supervisory function within the trading unit, namely front office supervision (FOS), to oversee trading activities. The FOS function was responsible for carrying out day-to-day controls and monitoring to detect and prevent operational risks, staff misconduct and non-compliance issues.

    (ii) The second line of defence refers to independent risk management and compliance functions. These functions are responsible for undertaking risk identification and assessment processes, managing firm-wide risk exposure and implementing controls and monitoring to ensure compliance with relevant regulations.

    (iii) The third line of defence refers to an independent audit function that assesses the effectiveness of the Group's operational risk management framework and ensures that risks identified are resolved.

Operational risk incident reporting and escalation

15. The Groups generally reported that senior management were provided with management information, such as incident reports and risk indicator monitoring dashboards, to oversee operational risk assessment and incident remediation processes.

16. When an operational risk incident occurred, most Groups would review the event chronology, identify the root cause (eg, deficiencies in internal controls or system failures) and assess the extent of the impact on their clients, the market and the firm. Based on the results of the review, these Groups would act to remediate the impact and formulate necessary measures to prevent a recurrence, such as enhancing their internal controls and providing refresher training to staff. These Groups also put in place a written protocol for reporting operational risk incidents to senior management and, where the incident is material or involves regulatory breaches, to regulatory authorities.

17. Areas for improvement

    - A Group did not clearly set out the escalation requirements for operational risk incidents (eg, thresholds and timelines for escalation) in its internal policies. For another Group, the trading staff did not adhere to the timeline for reporting operational risk incidents as prescribed in the internal policies. These practices may undermine the effectiveness of management oversight and impede the prompt implementation of remediation plans.

Good practices
▪ Some Groups developed a matrix to facilitate the assessment of risk incidents (based on their nature, severity and financial impact) and their escalation to appropriate levels of management. Incidents assessed as high risk (including those with significant client, financial, reputational or regulatory impact) would require more prompt attention from upper-level senior management (eg, immediate escalation to the chief executive officer).

Fostering a risk culture

18. Risk culture refers to the degree to which risk governance is accepted at all levels of the organisation[5]. It is integral to the effective implementation of the firm's risk management framework.

19. The senior management of most Groups were aware of the importance of setting the right tone from the top to model staff behaviour, emphasising honesty, integrity and responsible risk management.

20. Some Groups provided supervisory guidance and training to staff to promote their risk awareness.

21. Some Groups appraised staff performance by giving consideration to their compliance history and applied incentives and penalties suitably to guide staff behaviour.

(b) Ongoing review of operational risk management framework

22. Most Groups performed periodic reviews of the adequacy and effectiveness of their risk management frameworks, including operational controls (see Part II of this section), at least annually. Ad hoc reviews would also be performed when changes were made to the risk profiles of trading activities (eg, after new product launch) or when operational loopholes were identified from risk incidents.

23. To facilitate their ongoing review of the operational risk management framework, the Groups generally used one or more of the following tools.

- Risk and control self-assessment (RCSA) – This involves a comprehensive assessment of the Groups' operational risk exposure and an evaluation of the effectiveness of their existing controls. This allows the Groups to formulate enhancements at an early stage to address any new types of risk or potential control loopholes identified. RCSA is often carried out by the FOS function and validated by an independent function (eg, risk management), and the results are presented to senior management for endorsement of any risk mitigation plans.

- Key risk indicators (KRIs) – The use of KRIs involves tracking and analysing the trends and impact of various risk factors, eg, repeated limit breaches or abnormal profit or loss movements. The Groups adopted KRIs to monitor the performance of

[5] More information about risk culture can be found in the SFC's report, "Risk-focused Industry Meeting Series: G-SIFI Trends in Risk and Risk Mitigation", published in December 2013.

operational controls under their risk management frameworks. Regular KRI reports, together with the relevant trade details, were presented to senior management for resolution of the potential need to tighten controls, conduct further investigations or take disciplinary action on non-compliant matters.

- Scenario analysis – These Groups conducted regular scenario analyses to assess the resilience of their existing risk management frameworks to potential operational risk events. They made use of internal models, with data from historical or hypothetical operational risk events (eg, losses from error trades), to project potential operational losses.

24. Areas for improvement

- A Group solely followed the group-wide operational risk management framework without conducting any review at the firm level to ensure that the framework is adequate and effective to prevent and mitigate operational risks stemming from local circumstances (eg, risk of breaching local short-selling requirements).

- A Group relied on KRIs as a risk monitoring tool to identify areas with high operational risk but did not conduct sufficient ongoing assessments of the appropriateness and effectiveness of the thresholds used in its KRIs. In one instance, the alert level for trading an over-the-counter (OTC) product was not commensurate with its historical trading volume. The Group acknowledged an error in setting the threshold, which was only identified upon our enquiry.

II. Operational controls and monitoring

25. Operational controls and monitoring herein refer to internal control measures implemented to detect and prevent errors, omissions or misconduct in trading activities which may result in financial losses or other harm to an LC. They are typically implemented at the pre-trade or post-trade level for an LC to ensure adherence to its risk appetite, trading and client mandates and regulatory requirements.

Expected standards
LCs should establish appropriate operational controls and monitoring[6] practices to detect and prevent errors, omissions or misconduct in their trading activities. They should ensure: (a) pre-trade and post-trade controls and monitoring are properly implemented and regularly reviewed and calibrated so that their trading activities comply with regulatory requirements and are in line with their risk profiles; and (b) trade exceptions identified from the operational controls and monitoring processes are properly assessed and followed up so that appropriate action could be taken at an early stage to mitigate any operational loopholes or misconduct in trading activities.

[6] General Principle 3 and paragraph 4.3 of the Code of Conduct and Part VIII and paragraph 35 in the Appendix of the Internal Control Guidelines.

Market practices

(a) Pre-trade and post-trade controls and monitoring

26. Most Groups deployed manual or automated controls and monitoring at the pre-trade or post-trade level, and sometimes both, to ensure adherence to trading mandates, trading and position limits and applicable regulatory requirements.

Examples of operational risk indicators addressed by trade controls and monitoring	
At pre-trade level	**At post-trade level**
▪ Breaches of trading and position limits ▪ Trading in restricted products or markets or with restricted counterparties ▪ Unauthorised trading in breach of trading mandates ▪ Uncovered short-selling of stocks ▪ Order input errors (eg, orders at an off-market price, repeated orders)	▪ High utilisation of trading and position limits ▪ Unusual trade amendments or cancellations ▪ Unusual trading patterns and outliers ▪ Trades with abnormally large volumes or sizes ▪ Unapproved or unjustified overrides of pre-trade controls

27. For automated controls and monitoring, the relevant Groups designed different system responses for various types of trade exceptions when pre-defined criteria and thresholds are reached.

- Alert warning or soft block – The order entry will be put on hold and could be processed when the relevant risk alert is acknowledged, justified and approved by relevant staff. This response is commonly adopted to alert staff of the entry of potentially erroneous orders (eg, order size exceeding current available funds or a repeated order); and

- Hard block – The order entry will be blocked completely. This response is commonly adopted to prevent the entry of an order that is not compliant with the regulatory requirements (eg, an uncovered short-selling order) or trading and client mandates (eg, an order for restricted products).

28. Areas for improvement

- Some Groups did not conduct regular reviews to ensure trade controls are comprehensively applied to all trading activities (eg, including those involving OTC derivatives (OTCD)). This increases the risk that unusual trading patterns and outliers indicative of excessive risk-taking may not be identified in time or at all.

- A Group implemented a pre-trade control to prevent uncovered short selling by checking clients' sell orders against their available stock balances. However, it was unable to identify in a timely manner a system limitation involving a delay in reflecting the reduction in clients' stock balances due to share consolidation or stock withdrawal. This gave rise to multiple incidents of settlement failures caused by trading staff inadvertently over-selling stocks for their clients.

(b) Handling of trade exceptions

29. Most Groups had in place a protocol for the review and handling of trade exceptions identified from their pre-trade and post-trade controls and monitoring (eg, trading mandate breaches, trade reconciliation issues and trading errors). Exceptions were initially assessed by the first line of defence (eg, the FOS function) in respect of the staff trading behaviour, root cause of the breach and client impact. The second line of defence (eg, the risk management function) would require trading staff to take remedial action in a timely manner and provide a reminder or warning afterwards to the relevant trading staff to prevent the breach from recurring. The compliance function may be involved to assess the regulatory impact and consider the need to report to regulatory authorities.

30. Some Groups also had an independent team to conduct quality assurance reviews to ensure that all trade exceptions were properly handled with adequate audit trails.

31. Areas for improvement

- Despite frequent and repeated breaches of the trading mandate where the trading of unapproved products caused unexpected losses, a Group did not take appropriate follow-up action such as initiating an assessment of the conduct of relevant trading staff and implementing enhanced controls to prevent the recurrence of those types of breaches. This may undermine the effectiveness of trade controls and cause connivance at non-compliant practices.

Good practices
▪ A Group conducted a review of trade exceptions (eg, unusual trade cancellations and amendments) not only through understanding the justifications provided by relevant trading staff and assessing the impact on profit or loss, but also through analysing risk indicators from the trading staff's past trading and compliance records, in order to uncover any irregularities indicative of more severe operational loopholes and to prevent further breaches.

C. Remote booking risk management for trading activities

Background

32. Remote booking typically refers to a business model where a trade originating or executing entity transfers the trading risks (eg, market or credit risk) to an offshore risk-booking affiliate through a group-wide remote booking arrangement. In turn, the risk-booking affiliate enters into a transfer pricing arrangement with the trade originating or executing entity to share the costs, profits or losses.

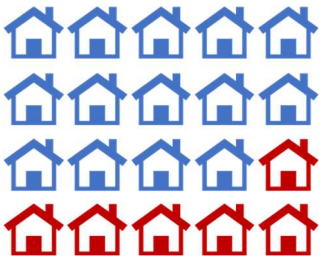
33. Out of the 48 selected Groups, 20 reported having a remote booking arrangement in place which enabled them to centrally manage the risks of trade portfolios (eg, through trade netting[7] and hedging[8]) at the risk-booking affiliates and efficiently manage the capital of group affiliates. This also came with a transfer pricing arrangement for these Groups to facilitate cost-sharing or profit or loss allocation amongst group affiliates.

Remote booking models

34. Two types of remote booking models are adopted by these Groups.

- Direct booking model – Trades are directly booked to an offshore risk-booking entity. The risk-booking entity, but not the trade originating or executing entity, is the contracting party facing the trade counterparties, and the credit risk[9] and market risk[10] arising from the trades would reside with the risk-booking entity.

- Back-to-back booking model – Trades are initially booked to the trade originating or executing entity. The trade originating or executing entity is the contracting party facing the trade counterparties. It would retain the credit risk of trade counterparties, but transfer the market risk arising from the trades to an offshore risk-booking entity by means of mirrored back-to-back transactions.



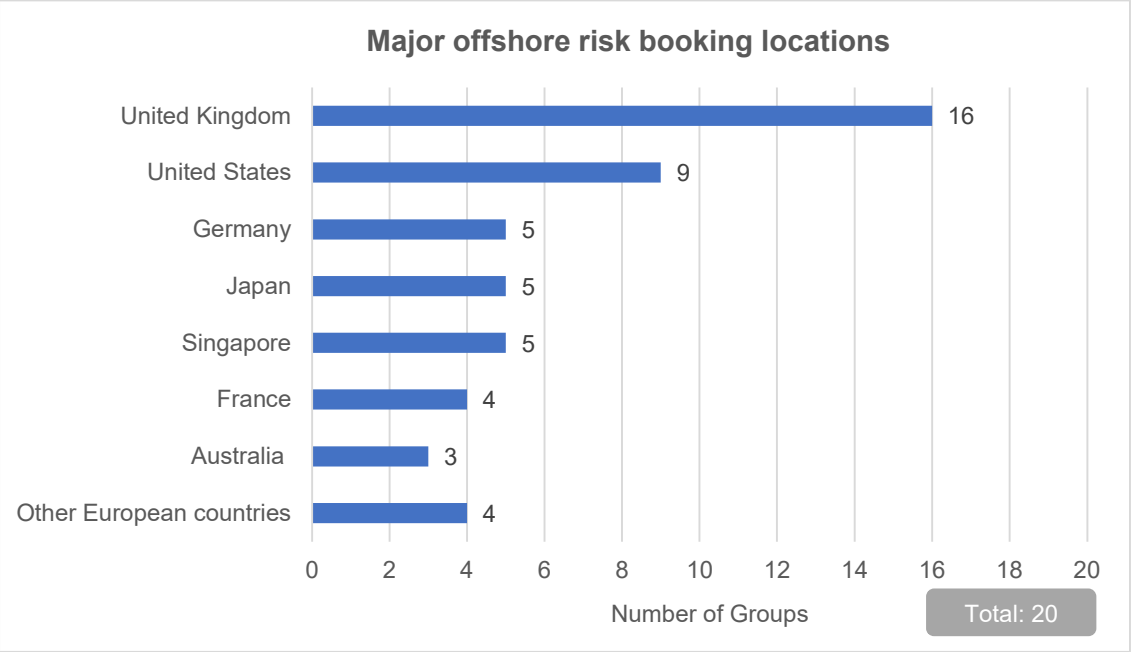
14 / 20 Groups solely adopting direct booking model.

6 / 20 Groups adopting both direct booking and back-to-back booking models.

[7] Netting is an arrangement to offset risk exposure by combining opposite trade positions in the same underlying asset.
[8] Hedging is an arrangement to offset risk exposure by taking opposite trade positions in the same underlying asset or another asset with high correlation.
[9] Credit risk is the risk that a counterparty may fail to perform an obligation owed to the firm.
[10] Market risk is the risk that movements in prices or values may result in loss for the firm.

Risk-booking locations

35. The diagram below shows the major offshore risk-booking locations used by the 20 Groups[11] (ie, the offshore locations where the risks of trades are remotely booked by LCs in Hong Kong). The most preferred locations were the United Kingdom and the United States. The 20 Groups indicated that the main factors determining the choice of a particular risk-booking location were (i) where the group or regional risk management function is located, and (ii) which regulatory capital regime imposes less onerous capital requirements for trading activities. Post-Brexit, some Groups migrated their risk-booking locations from the United Kingdom to European countries such as Germany and France.



36. Some Groups reported that trades originating from or executed by overseas affiliated entities could be booked in Hong Kong but the volume was low compared to the number of trades originating from or executed by LCs in Hong Kong and booked to overseas affiliates. The thematic review mainly focused on the risks faced by LCs as a trade originating or executing entity under remote booking arrangements.

I. Remote booking risk governance

37. Remote booking arrangements often involve multiple group affiliates and processes across different jurisdictions. The risk allocation and financial connections with group affiliates could be complicated. LCs must implement adequate risk governance to ensure that a robust management structure and proper group-wide coordination are in place to address the risks underlying remote booking arrangements (see paragraphs 47-48 for details).

[11] A Group may have one or more risk-booking locations.

Expected standards
LCs should have a sound risk governance framework[12] for remote booking arrangements. The framework should cover the following areas, amongst others: (a) clear definition of the responsibilities and accountability[13] of senior management for managing the underlying risks of remote booking arrangements; and (b) a mechanism to coordinate with group affiliates the development of risk management policies and the assessment of potential risks associated with remote booking arrangements (eg, build-up of risk exposure or booking failures).

Market practices

(a) Senior management's oversight and responsibilities in remote booking risk management

38. The Groups designated the MIC of Risk Management function and MICs of other functions (eg, Overall Management Oversight, Key Business Lines, Finance and Accounting, Operational Control and Review, Compliance) to oversee the remote booking arrangement, including the handling of risk incidents.

39. The senior management of these Groups held regular meetings to review their trading risk exposure under the remote booking arrangement and the root causes of risk incidents (eg, a delay or failure in booking trades to affiliates) and the progress in handling them as well as to discuss the impact of business development (eg, new product launch) on existing remote booking arrangements.

40. Areas for improvement

- A Group did not define the protocol and timeframe for escalating material trade booking incidents. In one instance, a member of its trading staff failed to book trade positions to a group affiliate under the remote booking arrangement. However, this incident was escalated to the relevant management committees only after eight months, which hindered the Group from making timely control enhancements to close the operational loophole.

(b) Coordination with group affiliates on remote booking operations and risk management

Group-wide governance forums or committees

41. The Groups generally considered that a structured communication protocol for the affiliates involved in remote booking arrangements was an effective means to enhance the transparency of the Groups' risk management processes and refine their risk strategies.

[12] General Principle 9 and paragraph 14.1 of the Code of Conduct and Part I of the Internal Control Guidelines.

[13] Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management issued by the SFC on 16 December 2016.

42. Some Groups held periodic governance forums at the group, regional and/or local levels to discuss and coordinate any remote booking matters (eg, excessive trading risk exposures or booking failures or errors).

43. Areas for improvement

- Some senior executives of a Group serving as core members of the group-level management committee that coordinated remote booking matters were absent from a number of the committee meetings where discussions of material trade booking issues related to the Group (eg, booking trades to an incorrect offshore trading book) were on the agenda. This calls into question their commitment to fulfilling their responsibilities to coordinate with group affiliates and resolve potential risk issues.

Good practices

- Some Groups which are trade-originating entities in a group-wide remote booking arrangement conducted frequent meetings with the offshore risk-booking entities to discuss and resolve trading and booking matters (eg, booking of trades involving breaches of trading mandates[14], utilisation of market risk limits and reconciliation of profit or loss allocations) which may have risk implications for both the trade-originating and risk-booking entities.

Policies and procedures

44. In general, the Groups' risk management hubs set up group-wide frameworks and coordinated with local risk management teams to lay down local policies to govern remote booking arrangements.

45. These policies and procedures normally covered the risk management roles and responsibilities of senior management and relevant functions, escalation procedures for risk or booking incidents and controls and monitoring to ensure the effective operation of remote booking arrangements.

46. Areas for improvement

- Some Groups relied only on group-level policies governing remote booking arrangements. These policies did not sufficiently define senior management's responsibilities and accountability in the local context. Also, the escalation procedures for remote booking incidents and the authority for setting local risk limits both lacked clarity.

II. Remote booking controls and monitoring

47. Under a group-wide remote booking arrangement, LCs can remotely book trades and hence transfer risks to their group affiliates. If LCs fail to properly book trade positions to group affiliates due to operational issues (eg, booking of trades without an authorisation or exceeding pre-defined limits), the losses incurred might reside with the LCs.

[14] Refer to Section (C)(II) below for more details of trading mandates.

48. In addition, LCs involved in group-wide transfer pricing arrangements may be allocated costs or trading losses by group affiliates from time to time. If the allocated losses are disproportionately or unexpectedly large, LCs could face imminent financial risk.

Expected standards
LCs should ensure that appropriate controls and monitoring[15] are implemented to manage the risks arising from remote booking arrangements with their group affiliates[16]. The controls and monitoring should cover the following areas, amongst others. **(a) Controls and monitoring for booking positions to group affiliates** (i) **Trading mandates** – LCs should establish trading mandates to clearly set out the responsibilities and authority of trading staff, including the trading and booking activities to be conducted under remote booking arrangements. Appropriate controls and monitoring should be implemented to ensure their staff's adherence to trading mandates. (ii) **System access controls** – LCs should implement appropriate system access controls to ensure that only authorised personnel conduct remote booking activities. (iii) **Risk limits** – LCs should ensure risk limits are in place to control and manage the trading risks they undertake. Appropriate controls and monitoring should be implemented to ensure their staff's adherence to risk limits. **(b) Loss allocation controls and monitoring for transfer pricing arrangements** LCs should implement adequate controls to monitor the size of any losses to be allocated to them under transfer pricing arrangements and take appropriate measures to prevent material loss allocation which may impair their financial capability.

Market practices

(a) Controls and monitoring for booking positions to group affiliates

Trading mandates

49. All the Groups established trading mandates to define the trading and booking activities to be undertaken by their trading units or staff as part of the remote booking

[15] General Principle 3 and paragraph 4.3 of the Code of Conduct and Part VIII of the Internal Control Guidelines.

[16] LCs should comply with: (i) paragraph 20.1 of the Code of Conduct regarding risk management standards when there are financial exposures to group affiliates and (ii) paragraphs 20.3 to 20.5 of the Code of Conduct when LCs book OTCD transactions to group affiliates which are not regulated in a comparable OTCD jurisdiction.

arrangements. The mandates may include a list of permitted products and the Group's trading and hedging strategies.

50. For any update to the trading mandates, most Groups had in place a mechanism that required the approval of more senior supervisory staff in the trading unit, an independent function (eg, risk management or compliance) or both for mandates entailing higher risk exposure.

51. Some Groups required their FOS function to monitor the compliance of staff with trading mandates.

52. Areas for improvement

- A member of the trading staff of a Group was assigned excessive authority for booking trades to group affiliates, including types of products which were beyond his trading mandate. However, the Group did not discover this in a timely manner due to the lack of a review mechanism. This staff member inadvertently conducted multiple trades in breach of his trading mandate.

System access controls

53. Most Groups granted system access rights to their staff for conducting remote booking activities on a need basis. For instance, trading staff and their supervisors were granted "read and write" access, ie, they were allowed to view trading positions and book trades or transfer risks offshore, whereas staff who only needed to view the trading positions for monitoring purposes (eg, risk management and compliance) were granted "read-only" access.

54. Some Groups required their FOS function to perform periodic reviews of trading book access rights to ensure that they remained appropriate.

55. Some Groups also put in place detective controls to identify any unauthorised access to the trading books.

56. Areas for improvement

- A Group's FOS function discovered that access rights of a member of its trading staff for booking trades to an offshore group affiliate were no longer needed, but the rights were only removed from the system after a long time. The Group could have been exposed to the risk that unauthorised booking of trades to offshore entities could occur without detection during that period.

Risk limits

57. In general, the Groups had risk limits in place for managing the risk exposures of their remote booking activities at various levels (eg, individual trading staff, trading desk, entity and group levels) and they monitored adherence to risk limits on an ongoing basis.

58. Some Groups deployed automated controls (eg, system alerts to trading staff and risk management teams) to help detect the high utilisation rates of risk limits during the day,

while some Groups utilised exception reports to capture risk limit breaches at the end of the day.

59. Some Groups allowed trading staff to apply for a temporary uplift of risk limits subject to the approval of supervisors or the FOS function. They required documentation of the details of the risk limit uplift, including its size, effective period and justification.

60. Areas for improvement

- A Group allowed its trading staff to execute orders beyond its internal trading limits based on certain justifications. However, in some instances, the required justifications were found to be either incomplete or absent. This would impair the effectiveness of any post-trade reviews conducted by the Group to assess whether the temporary uplifts of risk limits are reasonable and appropriate.

Good practices

- A Group established trading mandates and limits with automated system blocks and an alert mechanism for non-compliant trades to ensure that its trading and booking activities conformed to group-level risk management policies and remote booking arrangements. The Group regularly reviewed and validated the appropriateness of all its trading mandates and limits. When revisions were made, the Group required relevant trading staff to acknowledge the revised trading mandates and limits and commit to following them.

(b) Loss allocation controls and monitoring for transfer pricing arrangements

61. The 20 Groups with remote booking arrangements in place all adopted transfer pricing arrangements with their trade originating or executing entities and risk-booking entities.

62. In most cases, the transfer pricing arrangements required the risk-booking entities to bear trading losses. In other cases, they allowed the risk-booking entities to share trading losses with the trade originating or executing entities in whole or in part depending on the product type.

63. Most of the Groups with transfer pricing arrangements reported having written agreements to govern their implementation. To facilitate compliance with overseas and local tax reporting requirements, these Groups prepared transfer pricing documentation reports to document the value drivers, interdependence of the functions performed and risks borne by entities within the financial group.

64. Some Groups prepared an annual budget of their financial capacity taking into account the historical profit or loss allocation patterns under their transfer pricing arrangements and the forecast of any unexpected loss allocation (eg, due to the underperformance of group affiliates).

65. Some Groups established procedures to regularly monitor the exposure to and transfer of risks and evaluate the resulting impact. They also had a mechanism in place to monitor their liquid capital and escalate any financial risk to senior management in a timely manner.

66. Areas for improvement

- The losses to be allocated to a Group under a group-wide transfer pricing arrangement could be exceptionally large, which may result in its insolvency. However, the Group did not properly evaluate the related financial implications or take sufficient measures to address the risks.

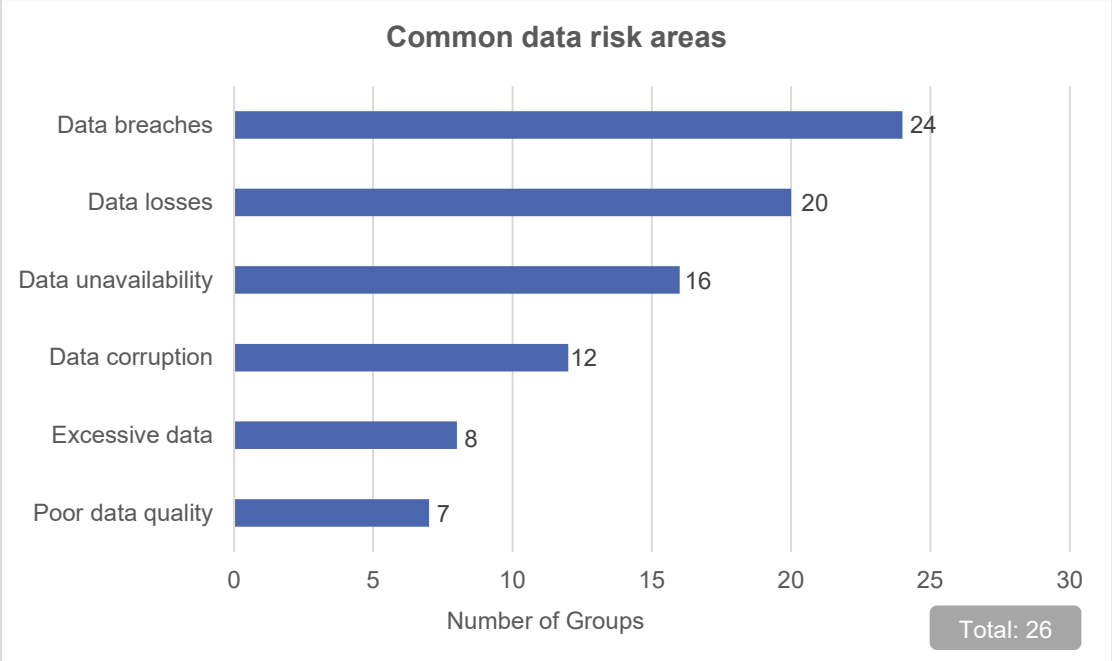
Good practices
▪ A Group had a contingent financial arrangement with overseas group affiliates which allowed a capital injection from its financial group or re-allocation of losses to other group affiliates in case of a potential material loss that reduces the Group's liquid capital to a precarious level.

D. Data risk management

Background

67. Data risk generally refers to the risk of operational disruptions and reputational or financial losses due to LCs' deficiencies in managing the data lifecycle, which includes the collection, classification, usage, retention, transfer and disposal of data.

68. Among the 48 Groups in the review, 26 reported that they had experienced incidents relating to data risk. The top three data risk areas[17] identified by these Groups were data breaches[18], data losses[19] and data unavailability[20]; other risk areas included data corruption[21], excessive data[22] and poor data quality[23].



69. Data risk is drawing mounting attention around the globe in light of the burgeoning volume of data collected and used in business operations. It is of paramount importance for LCs to exercise sufficient management oversight of data risk management, institute appropriate controls and monitoring at each stage of the data lifecycle and put in place adequate protection measures to safeguard data from being leaked, lost or compromised.

---

[17] In response to the questionnaire, the Groups were allowed to report one or more areas of data risk where relevant.
[18] A data breach is a security breach where confidential or sensitive data is stolen or processed without the authorisation of the data owners.
[19] Data losses refer to intentional or unintentional destruction of data.
[20] Data unavailability is a temporary loss of access to data at a specific time.
[21] Data corruption is damage which makes the data unusable.
[22] Excessive data refers to the unnecessary collection and processing of data which may give rise to privacy concerns.
[23] Poor data quality refers to incomplete, inaccurate or inconsistent data.

I. Data risk governance

70. A robust risk governance structure, coupled with well-defined risk management roles and responsibilities, is critical for LCs to respond promptly to data risks stemming from their business practices and the emergence of new technology, 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.

Expected standards
LCs should put in place a sound risk governance framework[24] for the effective management of data risks and compliance with the applicable legal and regulatory requirements[25]. The framework should cover the following areas, amongst others: (a) clear definition of senior management's responsibilities and accountability[26] 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.

Market practices

(a) Senior management oversight of and responsibilities for data risk management

71. Most Groups put in place a data risk governance framework for management oversight and the escalation of incidents related to data risk. The written frameworks mainly set out the roles and responsibilities of designated officers (eg, the MIC of Risk Management function, MIC of Information Technology function) and committees for overseeing data risk management and ensuring the implementation of controls and monitoring throughout the data lifecycle.

72. Senior management of most Groups acknowledged the importance of raising staff awareness of data risk issues and compliance with data risk related policies, by such means as induction and periodic training on how to handle sensitive information and report data risk incidents.

73. Areas for improvement

- Without an adequate understanding of data risks, some Groups were unable to clearly delineate management responsibilities. For example, it could be unclear whether the MIC of Risk Management function, the MIC of Information Technology function or both should oversee data risk and related incidents.

[24] General Principle 9 and paragraph 14.1 of the Code of Conduct and Part I of the Internal Control Guidelines.
[25] Including the PDPO.
[26] Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management issued by the SFC on 16 December 2016.

Good practices

- Some Groups designated a data governance committee comprising representatives from information security or data management, compliance, legal and operational risk functions. The committee oversees the implementation of the data risk management framework as well as controls for the identification and handling of data risk issues. Management reports on significant data-related issues were provided to the committee and discussed in periodic committee meetings.

(b) Handling of data risk incidents

74. While most Groups designated officers or committees to which material data risk incidents would be reported within a prescribed timeframe, some Groups also formed special task forces to expedite the process for identifying the root causes of these incidents and mitigating the risk exposure after they occurred. A special task force may be composed of different stakeholders (eg, heads of key business lines and information technology, risk management and compliance functions) depending on the nature and severity of the incident.

75. In cases of data loss or leakage, the responsible parties within these Groups would generally assess the potential impact, determine appropriate measures for containing the pertinent risks and take care of any necessary reporting to fulfil legal and regulatory obligations.

76. Areas for improvement

- Some Groups did not clearly define escalation protocols and timeframes. Some incidents (eg, data loss) were not reported to senior management in a timely manner and this undermined the effectiveness of management oversight.

Good practices

- Some Groups adopted a centralised system to track the progress of their responses to data risk incidents and implement remedial measures in a systematic way. This can facilitate monitoring by relevant independent functions and reporting to senior management.
- A Group performed an annual drill with its staff to simulate the occurrence of data risk incidents, familiarise staff with the incident handling and escalation protocol and evaluate the effectiveness of its processes.

II. Data lifecycle controls and monitoring

77. Appropriate controls and monitoring[27] are essential to manage the data lifecycle and mitigate the associated risks[28] which may stem from poor data quality, unauthorised data access or leakage or loss of sensitive data.

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

(a) Data collection

78. LCs rely heavily on quality data to make business decisions and conduct business operations.

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

Market practices

79. When collecting data for specific business purposes, such as fulfilling know-your-client requirements, performing market research and analysing staff behaviour, the Groups generally observe the PDPO and other applicable laws and regulations.

80. The Groups obtained information and data from a variety of sources. In general, the Groups obtained clients' prior consent and disclosed to clients the purpose of data collection before accessing any client data. Most Groups sought to obtain other types of data, including market data, from authorised, reliable sources such as commercial databases.

81. Some common approaches adopted by the Groups to ensure data quality include assessing the reliability of data sources (eg, due diligence on data providers) and carrying out risk-based data validation (eg, verifying the accuracy and completeness of critical data).

(b) Data classification

82. Under a risk-based approach, LCs often identify sensitive data and deploy heightened safeguard measures to prevent their loss or leakage.

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

Market practices

83. The Groups established processes to classify data based on the level of sensitivity and associated risks. Common data categories include "highly confidential", "confidential", "internal" and "public".

---

[28] LCs which engage in internet trading should also make reference to the guidance set out in the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading and the good practices set out in the Circular to Licensed Corporations Regarding Good Industry Practices for IT Risk Management and Cybersecurity issued by the SFC on 27 October 2017, as well as the additional guidance set out in the Report on the 2019-20 thematic cybersecurity review of internet brokers issued by the SFC on 23 September 2020, in relation to data protection measures against cybersecurity risk.

84. Data classification serves to facilitate the Groups' formulation of controls with pertinent risk-based considerations. In general, the Groups had enhanced safeguards for confidential data, such as data encryption, data masking[29] and physical and logical[30] access controls.

85. Some Groups further implemented systems to protect and secure data in various endpoints, networks and communication channels such as email and shared drives. Within these systems, the Groups established rules or criteria to detect any unauthorised transfer of data or any sensitive information contained in the communications, and applied soft or hard blocks on data transmission (eg, outgoing emails) as appropriate. When these systems identified alerts, designated teams would review them and determine whether data leakage occurred and whether escalation to senior management was required.

(c) Data usage

86. Access controls are key to restricting data usage to appropriate personnel and external parties authorised by the LCs, and to detecting and preventing unauthorised data access.

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

Market practices

87. To avoid unauthorised usage of data, most Groups granted data access to their staff on a need basis in accordance with the confidentiality categories. Access controls and monitoring mechanisms were also implemented to ensure that only authorised persons can access and use relevant data.

88. Some Groups maintained records of the inflow and outflow of confidential information for each department. These records included descriptions of the information, data owner, data receiver and confidentiality level, and were reviewed by a designated department to identify any mishandling of confidential data.

89. Areas for improvement

- A Group stored all unpublished research materials, which were classified as "confidential" data, in a shared drive and did not restrict access only to staff on a need basis. Without appropriate access controls, price-sensitive information contained in research materials could be prone to leakage and misuse before publication.

[29] Data masking is a technique to protect sensitive data by hiding or modifying the original data.
[30] Logical access controls involve the identification, authentication and authorisation of personnel for system access (eg, with the use of passwords or biometrics).

(d) Data retention

90. To address both regulatory expectations and business needs, LCs need to determine the appropriate retention periods and storage media for various types of data.

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.

Market practices

91. The Groups generally set the minimum retention periods for different types of data, such as personally identifiable information and transaction data, in order to fulfil business needs and regulatory requirements.

92. Most Groups retained confidential data, such as client, transaction and employee information, in an encrypted storage medium.

93. Apart from in Hong Kong, some Groups also retained their data in multiple offshore locations, particularly where their group companies operated to fulfil group-wide data backup and business resilience requirements.

94. Areas for improvement

- Some Groups did not set a minimum retention period for some types of data (eg, clients' personal information obtained from the know-your-client process or other business operations), leading to the premature disposal of records which are required to be kept under the Securities and Futures (Keeping of Records) Rules.
- Some Groups retained records of clients' personal data permanently, even though the clients' accounts may have been closed for more than a decade and the records were no longer required for regulatory record-keeping purposes. This may not be in line with the PDPO[31], which requires all practicable steps to be taken to erase personal data that is no longer required.
- For some Groups, safeguards for the proper retention of confidential documents were insufficient. A number of client or internal records were missing either because their staff misplaced them or backup processes failed, resulting in breaches of the Securities and Futures (Keeping of Records) Rules.

[31] Data Protection Principle 2 – Accuracy and duration of retention of personal data.

(e) Data transfer and disposal

95. LCs need to be vigilant to address the higher risk of data loss and leakage when transferring[32] and disposing of data.

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.

Market practices

96. Most Groups reported that data transfer occurred within the firm and with third-party service providers and group affiliates in and outside Hong Kong. Data may be shared through emails, external portable storage, shared drives or system interfaces. Encryption is the most common way to secure the data transfer process.

97. Some Groups blocked the installation of unauthorised software and hardware (eg, USB devices and external hard disks) on their computer systems. Some Groups also implemented data loss prevention software to mitigate the risk of data leakage or loss due to internal or external factors.

98. When disposing of sensitive data, the Groups generally shredded data or information in paper form so that it was no longer readable. Media destruction and degaussing were the common methods to destroy electronic data.

99. Some Groups required the sensitive data disposal process to be monitored by a designated function (eg, compliance) or a third-party service provider.

100. To determine when data should be disposed of, some Groups referred to the internal record retention schedule for different types of data. These Groups assigned staff to conduct periodic reviews to evaluate whether the schedule was up-to-date, and whether the data had been properly disposed of in accordance with the schedule.

101. Areas for improvement

- Some Groups' employees sent emails containing highly confidential data (eg, client or proprietary information) to their personal email accounts prior to employment termination, but the Groups lacked adequate control measures for the effective and timely detection or prevention of this kind of data leakage.

[32] LCs should also pay attention to the Circular to Licensed Corporations Regarding Managing the Risks of Business Email Compromise issued by the SFC on 24 March 2022 for implementing appropriate control measures to avoid leakage of client information.

(f) Use of third-party service providers

102. When LCs engage third-party service providers[33] to perform certain activities in the data lifecycle and the service providers have access to LCs' proprietary and sensitive data, the LCs are highly exposed to risks and vulnerabilities.

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.

Market practices

103. Some Groups reported that they engaged third-party service providers to carry out certain activities as part of the data lifecycle. These Groups performed due diligence and ongoing reviews of service providers' control environments to ensure they put in place adequate data protection measures.

104. The transfer of data was generally bound by service-level agreements between these Groups and their third-party service providers, particularly for handling confidential information and data disposal upon termination of service. The service-level agreements set out the responsibilities of the relevant parties, ownership of the data and compliance requirements.

105. Areas for improvement

- A Group engaged a third-party service provider to migrate confidential client data to new hardware, but did not conduct due diligence on the service provider's capabilities or ongoing monitoring of its service performance. This could expose the Group to higher risk of data leakage.

Good practices
▪ When terminating services, a Group instructed the service providers to dispose of the relevant data by following these measures: (i) assigning appropriate staff of the Group to witness and verify the data disposal; and (ii) requiring service providers to affirm that the relevant data was disposed of properly.

[33] LCs which use external electronic data storage providers to keep records required under the Securities and Futures Ordinance (Cap 571) or the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap 615) should also comply with the applicable requirements and expected regulatory standards set out in the Circular to Licensed Corporations Regarding Use of External Electronic Data Storage issued by the SFC on 31 October 2019.