A. Internal control and governance

Policies and procedures

Deficiencies and non-compliance

1. Some LCs' policies and procedures were not comprehensive enough to provide sufficient guidance for staff in implementing some critical AML/CFT controls for customer risk assessments, customer due diligence (CDD), transaction monitoring and sanctions screening, resulting in various deficiencies and non-compliance discussed in sections B to E below.

2. Some LCs failed to update their AML/CFT policies and procedures for a protracted period after amendments were made to the AMLO[1] and AML Guideline[2] in 2018, making them susceptible to contravening the new statutory and regulatory requirements.

Expected regulatory standards
LCs should put in place appropriate mechanisms to develop and continuously review their firms' AML/CFT policies and procedures to ensure that they are sufficiently comprehensive to ensure compliance with current statutory and regulatory requirements[3].

Example of good practices
An LC has mechanisms in place to review its AML/CFT policies and procedures on an annual basis and upon trigger events (eg, a change of regulatory requirements or an introduction of a new product) to ensure that they are up-to-date, meet current statutory and regulatory requirements and are effective in managing the ML/TF risks arising from all of its business activities.

Staff training

Deficiencies and non-compliance

3. Inadequate staff awareness of the reporting obligations and the offence of tipping-off under the relevant AML/CFT laws was observed in our inspections as illustrated by the following examples:

   (a) upon identifying suspicious transactions indicative of market misconduct, sales staff of an LC approached the customers concerned and warned them against conducting similar transactions, which might constitute an offence of tipping-off or disclosing information which is likely to prejudice an investigation; and

   (b) staff of an LC rejected a customer account application out of concerns about the applicant's possible involvement in fraud and tax evasion, but failed to consider the

[1] Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap.615).
[2] Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations).
[3] Paragraph 2.13 of the AML Guideline.

need to assess if there were grounds for suspicion of ML/TF for reporting to the Joint Financial Intelligence Unit (JFIU).

Expected regulatory standards
LCs should provide adequate training to staff to enhance their sensitivity to ML/TF red flags and help them understand and carry out their duties in accordance with the firm's policies and procedures including how to avoid tipping-off[4]. *LCs should note that their obligations to report suspicions of ML/TF apply even where no transaction has been conducted by or through the LCs. The tipping-off prohibition includes circumstances where a suspicion has been raised internally within the LC but has not yet been reported to the JFIU[5].*

Compliance monitoring and independent review

Deficiencies and non-compliance

4. Some LCs failed to put in place any—or adequate—ongoing compliance monitoring and periodic independent review arrangements to ensure the effectiveness and proper implementation of their AML/CFT policies, procedures and controls (AML/CFT systems). For instance:

   (a) an LC did not put in place any arrangement for continually monitoring the implementation and effectiveness of its AML/CFT systems apart from internal audit reviews carried out on a three-year cycle. Due to the limited scope and frequency of the internal audit review, a number of incidents of non-compliance by staff (eg, failure to carry out additional due diligence measures on customers which opened accounts using a non-face-to-face approach) went undetected for a protracted period until they were identified in the SFC's inspection; and

   (b) an LC relied upon its overseas affiliates to perform transaction monitoring of the orders its customers placed using the LC's direct market access account maintained with the affiliates, without implementing any measures to ensure that the affiliates performed transaction monitoring of these orders in accordance with the LC's requirements.

Expected regulatory standards
LCs should put in place effective compliance monitoring and independent review arrangements to monitor the implementation and effectiveness of their AML/CFT systems. The frequency and extent of monitoring and review should be commensurate with the nature and complexity of the businesses of LCs and enable the identification and rectification of deficiencies or non-compliance in critical AML/CFT controls in a timely manner. Where appropriate, LCs should seek a review from external parties[6].

[4] Paragraphs 7.9, 9.4 and 9.5 of the AML Guideline.
[5] Paragraphs 7.5 and 7.6 and footnote 55 of the AML Guideline.
[6] Paragraphs 2.13, 2.15 - 2.16 of the AML Guideline.

Example of good practices
An LC's AML/CFT systems are subject to ongoing monitoring by its compliance function to assess the level of compliance as well as to an independent review of their effectiveness by the group internal audit function on an annual basis. The work plan for compliance monitoring is developed and reviewed annually taking into account factors such as the regulators' requirements and recommendations, internal audit findings and the outcomes of institutional risk assessments and previous assurance and testing activities. The review results are communicated to the respective control function managers for them to respond and ensure remedial actions are properly implemented.

Senior management oversight

Deficiencies and non-compliance

5. Senior management of some LCs did not receive sufficient information for maintaining adequate oversight of the implementation of the firms' AML/CFT systems. Issues relating to the execution of critical AML/CFT controls, eg, the accumulated backlog of sanctions screening and transaction alerts pending for review, delays in the performance of periodic reviews of customer information, were not reported to senior management. Hence these issues were not addressed for a protracted period, exposing the LCs to increased ML/TF risks.

Expected regulatory standards
The senior management of an LC is responsible for implementing effective AML/CFT systems which can adequately manage the firm's ML/TF risks[7]*. Appropriate reporting mechanisms should be put in place for senior management to be apprised of key ML/TF risks and concerns in a timely manner and to enable them to take appropriate action to adequately manage and address them.*

Example of good practices
An LC has established mechanisms for regular reporting information to senior management for monitoring ML/TF risks arising from its business and the effectiveness of its AML/CFT systems. Examples of the information reported include analysis of customers on-boarded by ML/TF risk categories and specific risk factors as well as the volume and completion status of AML/CFT control procedures to monitor workload and whether these procedures are performed in a timely manner. Key AML/CFT issues, eg, significant compliance deficiencies, are promptly escalated to senior management for appropriate action.

[7] Paragraph 2.11 of the AML Guideline.

B. ML/TF risk assessments

Risk factors for assessing ML/TF risks

Deficiencies and non-compliance

6. Inadequate consideration of all key, relevant ML/TF risk factors in the institutional risk assessment (IRA) and customer risk assessment (CRA) processes was commonly observed in our inspections, as illustrated by the following examples:

   (a) Some LCs failed to adequately assess country risk according to the AML Guideline[8]. One LC only made reference to a list of jurisdictions identified by the Financial Action Task Force (FATF) as having strategic deficiencies in their AML/CFT regimes but did not consider other factors such as the level of corruption or connection to terrorist activities or organised crime which may pose higher risks. Another LC deemed all countries which are a member of a FATF-style regional body as non-high risk without conducting a proper assessment.

   (b) Some LCs failed to consider the potentially higher risks associated with certain products or services, eg, direct market access services which might be exploited to conduct manipulative or abusive transactions.

   (c) Some LCs failed to consider the ML/TF risks associated with non-face-to-face account opening when establishing business relationships with overseas customers.

   (d) Some LCs did not take into account the higher ML/TF risks associated with a customer's certain business, occupation or industry (eg, cash-intensive businesses) or ownership structure (eg, a structure with nominee shareholders or shares in bearer form).

Expected regulatory standards
An LC should consider all relevant risk factors, including country risk, customer risk, product/service risk, and delivery/distribution channel risk, in determining the ML/TF risks to which the firm is exposed as well as the ML/TF risks associated with a customer or proposed business relationship. It should take into account the list of non-exhaustive examples of indicators which may present lower or higher ML/TF risks provided in the AML Guideline[9], whenever relevant. It should also, for the purpose of risk assessments, include consideration of relevant reports and guidance issued by the FATF, inter-governmental organisations, governments and authorities[10] from time to time and any higher risk factors notified to LCs by the SFC[11].

[8] Paragraphs 4.13 of the AML Guideline provide guidance on jurisdictions posing higher risks.
[9] Paragraphs 2.3 - 2.8 and 3.5 of the AML Guideline.
[10] Including *Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report* published by the Government on 30 April 2018, and the *Risk-Based Approach Guidance for the Securities Sector published by the FATF* in October 2018.
[11] Including the SFC's circular dated 9 October 2018 on Use of "nominees" and "warehousing". arrangements in market and corporate misconduct, the SFC's circular dated 31 May 2019 on Third-party deposits and payments, and the SFC's circular dated 21 November 2019 on Dubious private fund and discretionary account arrangements or transactions.

Implementation of institutional risk assessment

Deficiencies and non-compliance

7. In our inspections we observed the following shortcomings in the IRA process which undermined the usefulness of the IRA results for senior management to implement adequate and appropriate AML/CFT systems to manage ML/TF risks.

   (a) The assessment of inherent ML/TF risks was not supported by quantitative parameters such as the number or percentage of high risk customers. Where these parameters were analysed, they only covered customers on-boarded in the recent past, and not the entire customer base.

   (b) An evaluation of the adequacy and appropriateness of existing policies, procedures and measures for mitigating the assessed inherent ML/TF risks was not performed to ensure that the firms' exposure to ML/TF risks was reduced to an acceptable level.

Expected regulatory standards
An LC should conduct IRA to identify and assess the ML/TF risks to which it is exposed[12]. It should consider both qualitative and quantitative information obtained from internal and external sources so as to obtain an in-depth and holistic understanding of its ML/TF risk exposures. Also, the firm should evaluate its existing AML/CFT systems to determine whether they are adequate and appropriate to reduce to an acceptable level its exposure to the inherent ML/TF risks it identifies, and develop an action plan for any necessary enhancements.

Example of good practices
During its IRA process, an LC supported its inherent ML/TF risk assessment by performing quantitative analyses of the number and percentage of high risk customers and the volume and value of cross-border transactions to and from high risk jurisdictions, among other factors, to gain an in-depth and holistic understanding of its ML/TF risk exposures. In evaluating the adequacy of its AML/CFT systems, the LC not only assessed whether or not policies and procedures were in place to manage the ML/TF risks identified, it also considered control testing results in internal audit reports, compliance self-assessments, reports by regulators, and conducted interviews and process walkthroughs with its relevant personnel. Based on the review results, the LC determined the firm's residual ML/TF risks and identified areas which warranted further attention and where improved controls were needed to further mitigate the risks.

Implementation of customer risk assessment

Deficiencies and non-compliance

8. It was commonly found that LCs provided insufficient guidance to staff on how to interpret and identify certain high risk factors, eg, involvement in "cash intensive business" or "sensitive or high risk activities" and use of "complex ownership structure" in relation to a

[12] Appendix 1 to the SFC's circular dated 31 August 2018 on AML/CFT measures and controls inspection findings.

CRA. This resulted in the assignment of different ML/TF risk ratings to customers with apparently similar risk profiles.

9. Other inconsistencies in CRA processes were noted where some LCs failed to:

   (a) properly follow the methodology and set of risk factors applied in the initial CRA process in the subsequent review and update;

   (b) ensure consistency in the risk ratings assigned to different accounts controlled by the same customer or beneficial owner; and

   (c) review whether any of their existing customers ML/TF risk levels should be elevated when the LC adjusts the country risk of a jurisdiction from non-high risk to high risk.

10. In some LCs, the basis for assessing a customer's risk level, including the risk factors considered and the supporting rationale, was lacking or insufficiently documented. This is a critical shortcoming. Customers were not rated as high risk notwithstanding the presence of high-risk factors such as connections with politically exposed persons (PEPs) or past involvement in financial crimes.

Expected regulatory standards
LCs should implement comprehensive policies and procedures to provide sufficient guidance to their staff to perform CRA properly. This may include, among other things, the requirement to obtain sufficient information to establish a customer's profile, explanations, with illustrative examples, of higher risk factors, and the requirement to keep proper records of CRA together with relevant supporting documents to demonstrate how the staff assesses a customer's ML/TF risks[13]. *In performing CRA, LCs should implement appropriate measures which ensure the application of a consistent CRA methodology, including the risk factors which must be considered, throughout the lifecycle of all business relationships (eg, the use of automated tools to calculate and verify a customer's risk score based on properly tested algorithms to minimise human errors or omissions).* *LCs should also review their existing customers' ML/TF risk levels whenever there are updates in the risk factors used in the CRA process, evaluate whether any of the existing customers should be moved to a higher ML/TF risk category and require additional measures to mitigate the risks identified.*

[13] Paragraph 3.8 of the AML Guideline.

C. Transaction monitoring and reporting

Transaction monitoring systems and processes

Deficiencies and non-compliance

11. The transaction monitoring systems and processes of some LCs exhibited the following critical shortcomings:

    (a) not all fund deposits by clients were assessed to ascertain whether they originate from third party payors and should be subject to the LCs' due diligence and transaction review processes;

    (b) monitoring was conducted at the transaction or account level without a holistic review of transactions across related accounts held by the same customers or beneficial owners;

    (c) the transaction monitoring rules were not properly calibrated by testing them to ensure they capture the transactions they were designed to capture.

Expected regulatory standards
LCs should regularly review the adequacy and effectiveness of their transaction monitoring systems and processes, including the parameters and thresholds adopted. LCs should ensure that these systems and processes can support the ongoing monitoring of a business relationship using a holistic approach, and the extent of monitoring should be commensurate with the customer's ML/TF risk profile[14]. The parameters and thresholds adopted in transaction monitoring should also be independently validated to ensure that they are appropriate for the LCs' operations and context[15].

Example of good practices
An LC conducts annual reviews of the scope and range of exception reports used for transaction monitoring to ensure adequate coverage of all of its business activities. Transaction monitoring rules for generating exception reports were tested and refined to ensure that they remain effective in identifying suspicious transactions and patterns, taking into account changes in business operations and developments in ML/TF methods. The assessment results and any enhancements to its transaction monitoring system are approved by senior management and properly documented.

Review of transactions, transaction alerts and internal reports

Deficiencies and non-compliance

12. A variety of deficiencies in detecting and following up on potentially suspicious transactions were noted.

[14] Paragraphs 5.6 and 5.9 of the AML Guideline.
[15] Paragraph 5.8 of the AML Guideline.

(a) An LC's trade monitoring system only focused on identifying suspicious transactions indicative of market misconduct and did not consider any indicators of other potentially suspicious transactions and activities associated with ML/TF.

(b) An LC accepted a customer's explanation for requesting a stock transfer by way of a bought and sold note that it was for a loan repayment and did not make further inquiries to understand the background and purpose of the transfer, assess reasonableness of the request or obtain corroborative evidence to validate the customer's explanation.

(c) An LC's Money Laundering Reporting Officer (MLRO) discounted an internal report concerning a customer's request for a cross-border fund settlement arrangement involving a tax haven country as not suspicious solely on the basis that the designated bank account used for settlement was in the customer's name. The MLRO did not take appropriate steps to ascertain the background and the purpose of the settlement arrangement in order to properly evaluate whether the arrangement was reasonable in the circumstances and consistent with the customer's profile.

13. There was a lack of documentation or insufficient documentation of the performance of transaction reviews as well as of the findings supporting the clearance of transaction alerts, and the rationale for concluding that a transaction which was flagged (or which should have been flagged) by some indicators of suspicious transactions used by the LC, or reported by staff to the MLRO, was not suspicious. Our inspections also identified failures to maintain records of internal reports verbally made to the MLRO. These shortcomings were considered critical as they would make it difficult for the LC, its auditors and the regulatory authorities to perform subsequent reviews of the adequacy of the LC's due diligence and evaluations of its review of transactions, transaction alerts and internal reports.

Expected regulatory standards
LCs should provide sufficient guidance and adequate training (which should be tailored to specific job functions and responsibilities) to all relevant staff to enable them to form suspicions or to recognise the signs when ML/TF is taking place, including the approach which staff may adopt (such as the "SAFE" approach promoted by the JFIU[16]) and the ML/TF red flags they should watch out for in customer transactions or their dealing with customers[17]. *LCs are reminded that the review of trading transactions should give due consideration to both potential ML/TF and market misconduct risks, and whether a report should be made to the SFC under paragraph 12.5(f) of the Code of Conduct[18], to the JFIU or to both.* *LCs should institute policies and procedures to ensure the findings and outcomes of transaction reviews, as well as the rationale for any decisions, are properly documented in writing to demonstrate how they have handled unusual or potentially suspicious transactions[19].*

[16] The "SAFE" approach promoted by the JFIU includes: (a) screening the account for suspicious indicators; (b) asking the customers appropriate questions; (c) finding out the customer's records; and (d) evaluating all the above information. Details of the "SAFE" approach are available at JFIU's website (www.jfiu.gov.hk).
[17] Paragraphs 7.10 to 7.15 and 9.4 to 9.5 of the AML Guideline.
[18] Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.
[19] Paragraph 5.17 of the AML Guideline.

LCs should implement clear policies and procedures which require proper records be kept of all internal reports made to the MLRO. The records should contain sufficient details of the customers concerned and the information giving rise to the suspicions as well as of the MLRO's deliberations and action taken which should demonstrate that the MLRO has acted in a reasonable manner[20].

Example of good practices

An LC sets out clear guidance in its policies and procedures for the review of transaction alerts, which requires staff to:

(a) consider all relevant information concerning the customer to which the alert relates, including obtaining further information and supporting documents from the customer as appropriate to understand the purpose of the transactions flagged in the alert and determine whether the transactions are commensurate with the customer's profile and background; and

(b) maintain sufficient documentation of the analysis performed as well as records of any decision, by whom it was made and the rationale for the decision.

The LC has also implemented maker-checker controls for the closure of alerts and quality assurance reviews of samples of the closed alerts to ensure the accuracy and appropriateness of the decisions.

[20] Paragraphs 7.19, 7.24 and 7.34 of the AML Guideline.

D. Implementation of CDD measures

Establishing source of wealth and source of funds

Deficiencies and non-compliance

14. The following critical shortcomings were noted in LCs' controls for establishing the source of wealth and source of funds for high-risk customers as required by the firm's policies and procedures, the AMLO[21] and the AML Guideline[22]:

    (a) Some LCs merely collected general financial information from high-risk customers in account opening forms and did not take reasonable measures to establish the source of wealth and source of funds.

    (b) An LC wrongly concluded that a customer's source of funds had been established after confirming that the funds were transferred from the customer's bank account without determining what activity generated the funds[23].

Expected regulatory standards
To establish a high-risk customer's source of wealth and source of funds, LCs should obtain relevant information from the customer and, using a risk-based approach, gather information from commercial databases and other available sources to verify the information provided by the customer[24].

Ongoing CDD procedures

Deficiencies and non-compliance

15. An LC should review CDD records on a regular basis (ie, periodically) and upon the occurrence of trigger events to ensure the documents, data and information remain up-to-date and relevant[25]. We observed that some LCs lacked or had inadequate mechanisms for identifying trigger events (eg, the reactivation of a dormant account). We also noted instances where the periodic reviews required by LCs' internal policies and procedures had been delayed for more than two years.

16. Another common shortcoming was that the review process was limited to negative news screening or reviews of customers' transactions against their historical profiles, without considering whether customers needed to provide confirmation or additional information to ensure that the information retained by the LCs was up-to-date and relevant.

Expected regulatory standards
LCs should implement clear policies and procedures for when to conduct a review of CDD information, including the frequency of periodic reviews and what constitutes a trigger

[21] Sections 10 and 15 of Schedule 2 to the AMLO.
[22] Paragraphs 4.9.2, 4.11.12 and 4.11.22 of the AML Guideline.
[23] Paragraph 4.11.14 of the AML Guideline.
[24] Appendix 2 to the SFC's circular dated 26 January 2017 on Compliance with AML/CFT Requirements.
[25] Paragraph 5.2 of the AML Guideline.

event, and provide sufficient guidance to staff on the scope of these reviews. Appropriate monitoring and supervisory measures should be put in place to ensure proper adherence to the firms' internal policies and procedures.

To ensure the CDD information retained by the LCs remains up-to-date and relevant, staff should review the veracity and adequacy of the CDD information previously obtained and when in doubt, take appropriate steps to confirm it with the customers and obtain additional information from them where appropriate[26]*.*

Example of good practices

An LC clearly defines in its policies and procedures the frequency of periodic reviews, what constitutes a trigger event and who in every business unit and support function having engagements with customers bears the responsibility for identifying a trigger event; the timeframe for completion of the CDD reviews, and the escalation and approval procedures when the CDD review cannot be completed within the specified timeframe. Guidance is provided to staff on the scope of the periodic review as well as the CDD review undertaken in response to a trigger event, which includes:

(a) confirming with the customer whether there are any material changes to the customer's information held by the LC and if so, updating the CDD records and documents;

(b) reviewing the customer's transactions since the last CDD review to assess whether they are consistent with the LC's knowledge of the customer's profile;

(c) name screening for the customer and its connected parties to identify connections with PEPs, sanctioned parties or adverse news; and

(d) *reviewing the customer's ML/TF risk level based on the updated information and requiring enhanced due diligence if the level is revised to high risk.*

[26] Paragraphs 4.1.9 and 5.2 of the AML Guideline.

E. Sanctions screening controls

Deficiencies and non-compliance

17. Some LCs' sanctions screening systems exhibited the following critical shortcomings:

    (a) an LC only performed sanctions screening of beneficial owners and other connected parties of customers at the time of on-boarding, and not during the ongoing sanctions screening process;

    (b) an LC wrongly believed that sanctions screening did not apply to low-risk customers such as listed companies, financial institutions and its own affiliated companies, shareholders and employees;

    (c) an LC had on-boarded investment managers which opened sub-accounts with the LC for each of the investment funds they managed. However, sanctions screening was performed only on the investment managers (the customer) and not on the investment funds (the beneficial owner on whose behalf the customer was acting); and

    (d) some LCs conducted ongoing screening of existing customers only at a fixed interval (eg, monthly or annually) without paying regard to new or updated designations promulgated in the meantime.

18. Other shortcomings which undermined the effectiveness of an LC's sanctions screening system included:

    (a) failure to ensure that screening alerts were reviewed on a timely basis, which resulted in a backlog of screening alerts pending for review;

    (b) failure to ensure that all screening results, including the justifications for disposing of any screening alerts, were properly documented; and

    (c) the automated screening system was inappropriately set to detect only exact name matches but not names with minor alterations, thereby increasing the risk of genuine hits being missed.

Expected regulatory standards
To avoid establishing business relationships with any terrorist suspects and possible designated parties, LCs should implement clear policies and procedures and effective screening mechanisms to ensure that, among other things: *(a) all customers are screened against current terrorist and sanctions designations when establishing a business relationship, and thereafter against all new and any updated designations as soon as practicable;* *(b) the screening must cover any beneficial owners of the customers and, using a risk-based approach, should extend to other connected parties and persons purporting to act on behalf of the customers;* *(c) screening alerts are reviewed in a timely manner to determine if possible name matches are genuine hits and a report should be made to the JFIU; and*

(d) the screening results and justifications for disposing of screening alerts are documented, or recorded electronically, to demonstrate that they have been followed up on and handled properly[27].

Where an automated screening system is used, LCs should ensure that the system setting is calibrated appropriately such that names with minor alterations (eg, reverse order, partial name, abbreviated form) can be reasonably detected, mitigating the risk of unwittingly dealing with terrorists or designated parties.

Example of good practices

To prevent terrorist financing and sanctions violations, an LC has established clear policies and procedures and provided adequate guidance to its staff who are responsible for performing sanctions screening to ensure that they are fully aware of the scope and coverage of sanctions screening and when it should be performed. The LC has also put in place maker-checker controls for the proper handling of screening alerts as well as monitoring procedures so that they are reviewed and resolved in a timely manner. It also adopts a fuzzy matching algorithm to increase the sensitivity of the automated screening system to detect possible name matches for appropriate scrutiny.

[27] Paragraphs 6.16 to 6.18 of the AML Guideline.