Appendix 1 – Deficiencies and inadequacies in meeting the expected regulatory standards

(A) Institutional risk assessment (IRA)

Deficiencies or inadequacies
➢ An LC mistook the completion of the AML/CFT self-assessment checklist[1] issued by the SFC as equivalent to the performance of an IRA. While the SFC's checklist is designed to provide a structured framework for LCs to assess their compliance with key AML/CFT requirements, it should not be used for other purposes such as identifying and assessing ML/TF risks to which LCs are exposed.
➢ An LC's IRA did not include an evaluation of whether its AML/CFT policies, procedures and controls were adequate and appropriate to address the identified ML/TF risks. This evaluation is necessary for the development of an action plan to enhance its AML/CFT policies, procedures and controls.
➢ Some LCs did not maintain records and relevant documents evidencing that their IRA results were reviewed and approved by senior management.

IRA is an important tool for an LC's senior management (including the Manager-In-Charge of the AML/CFT function) to fulfil their responsibilities to manage the firm's business effectively and ensure that its AML/CFT policies, procedures and controls are capable of addressing the ML/TF risks to which the firm is exposed[2].

During the IRA process, the LC should identify and assess the ML/TF risks to which the firm is exposed by considering all relevant risk factors including the products and services offered, delivery and distribution channels, types of customers and countries or geographical locations involved as well as analysing the firm's vulnerability to the ML/TF risks identified. The firm should evaluate the adequacy and appropriateness of its AML/CFT policies, procedures and controls to address those risks and develop an action plan for any necessary enhancements[3].

Senior management should review and approve the result of the IRA and any enhancement measures which are necessary to ensure the adequacy and appropriateness of the firm's AML/CFT policies, procedures and controls in light of the result[4], which should be supported by documentary evidence[5].

[1] See the SFC's AML/CFT self-assessment checklist: http://www.sfc.hk/web/EN/files/IS/AML/SELF_ASSESSMENT_CHECKLIST_ENG_2018.xlsx.
[2] Paragraph 2.11(a) of the AML Guideline.
[3] Paragraphs 2.2 to 2.8 of AML Guideline and Appendix 1 to the SFC's circular dated 26 January 2017 on Compliance with AML/CFT Requirements.
[4] Paragraph (c) of Appendix 1 to the SFC's circular dated 26 January 2017 on Compliance with AML/CFT Requirements.
[5] Paragraph IV.6 of the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission requires an LC to establish and maintain effective record retention policies to enable the firm, its auditors and other interested parties (including the SFC) to carry out comprehensive reviews.

(B) Customer risk assessment (CRA)

Deficiencies or inadequacies
➢ An LC failed to follow up on inconsistent information provided by customers (eg, a customer declared being unemployed but claimed a salary as his source of income) to ensure the conduct of adequate CDD.
➢ Some LCs failed to provide sufficient guidance to their management and frontline staff on how to determine a customer's overall ML/TF risk level based on a range of pre-defined risk factors. This resulted in inconsistent ML/TF risk levels being assigned to customers with similar risk factors.
➢ An LC allowed its relationship managers to override CRA results derived from the firm's assessment questionnaire without requiring that justification be provided.
➢ Some LCs did not maintain sufficient documentation to show how individual customers' ML/TF risk levels were derived. This undermined the effectiveness of any subsequent management or compliance reviews to ensure proper adherence to the firms' customer risk assessment policies and methodologies.

LCs should properly identify and categorise ML/TF risks at the customer level by considering all relevant risk factors, differentiate customers presenting a higher ML/TF risk and apply enhanced measures to manage and mitigate the risk[6].

LCs should provide sufficient guidance to staff and put in place adequate procedural and supervisory safeguards to ensure that they conduct CRA in compliance with the regulatory requirements and the firm's policies. LCs should, inter alia, ensure that their staff follow up on inconsistent information provided by customers to establish accurate customer profiles and require their staff to keep proper records of CRAs together with relevant documents to demonstrate how they assess individual customers' ML/TF risk levels[7].

[6] Paragraphs 3.1 to 3.3 and 3.5 of the AML Guideline.
[7] Paragraph 3.8 of the AML Guideline.

(C) Initial and ongoing CDD

(i)	**Deficiencies and inadequacies in initial CDD**
➢	CDD measures for corporate customers were inadequate: ▪ some LCs failed to obtain any reliable, independent source documents such as certificates of incorporation or certificates of incumbency to verify the identities of a corporate customer and its beneficial owners. ▪ some LCs failed to identify all beneficial owners (eg, individuals who ultimately own or control more than a 25% interest) of a corporate customer and verify their identities.
➢	An LC carried out name screening of customers against a commercially available database to identify politically exposed persons (PEPs). However, the scope of screening did not extend to the beneficial owners of the customers.
➢	An LC erroneously assumed that all customers which were collective investment schemes (CIS) were eligible for the application of the simplified CDD[8] under the AMLO without ascertaining whether the customers could meet the eligibility criteria for an investment vehicle to which the simplified CDD may be applied.
➢	An LC stipulated in its written policies and procedures that all high-risk customers were subject to enhanced CDD measures, but it did not elaborate or provide guidance on what measures should be applied in different scenarios. As a result, the CDD measures which were applied to high-risk customers varied depending on the personal judgement of frontline staff without any justification provided and did not comply with the special requirements under the AMLO for some types of customers.
➢	An LC did not implement any risk management policies and procedures for imposing conditions on continuing a business relationship with a customer when allowing the customer to utilise the relationship to effect securities transactions prior to the completion of identity verification.

It is a requirement under the AMLO that an LC must identify customers and verify their identities by using documents, data or information from reliable and independent sources, as well as identify and take reasonable measures to verify the identities of beneficial owners in relation to the customers. Beneficial owners in relation to a corporation include: (a) all individuals who own or control, directly or indirectly, more than 25% of the voting rights or share capital of the corporation; (b) any individuals who exercise ultimate control over the management of the corporation; and (c) any persons on whose behalf the customer is acting[9].

[8] Under section 4(1) of Schedule 2 to the AMLO, applying simplified CDD means that the beneficial owner of a customer is not required to be identified and verified.
[9] Section 1(1) of Schedule 2 to the AMLO.

An LC must establish and maintain effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP. The name screening procedures for the identification of PEPs must cover not only the customer, but also any beneficial owners of the customer[10].

Before applying the simplified CDD under the AMLO to a customer which is an investment vehicle (including a CIS), LCs should take appropriate steps to ensure that the customer meets the eligibility criteria[11], which should include:

(a) the LC is able to ascertain that the person responsible for carrying out CDD measures in relation to all of the investors of the investment vehicle falls within any of the categories of institutions set out in section 4(3)(d) of Schedule 2 to the AMLO[12]; and

(b) the LC is satisfied that the investment vehicle has ensured that reliable systems and controls are in place to conduct CDD on the underlying investors in accordance with requirements similar to those set out in Schedule 2 to the AMLO.

Depending on the customer's background and the product, transaction or service used by that customer, LCs should determine the extent of CDD measures using a risk-based approach and be able to demonstrate to the SFC that the extent of CDD is appropriate in view of the customer's ML/TF risks[13]. LCs should clearly define in their policies and procedures the enhanced CDD measures to be applied to their high-risk customers, which should match the nature and level of the customers' risks and comply with any applicable special requirements under the AMLO[14].

Before verifying the identities of a customer and any beneficial owners of the customer, LCs should not establish a business relationship with a customer unless associated ML/TF risks are effectively managed and the verification process is completed as soon as reasonably practicable. LCs should adopt appropriate risk management policies and procedures concerning the conditions under which this may occur, including:

(a) establishing timeframes for the completion of identity verification measures;

(b) monitoring such relationships regularly, pending the completion of the identity verification process, and keeping senior management periodically informed about any cases yet to be completed;

(c) obtaining all other necessary CDD information;

(d) ensuring that identity verification is carried out as soon as it is reasonably practicable;

(e) advising the customer of the LC's obligation to terminate the relationship at any time on the grounds of non-completion of the verification measures;

[10] Section 19(1) of Schedule 2 to the AMLO and Paragraph 4.13.9 of the AML Guideline.
[11] Section 4(3)(d) of Schedule 2 to the AMLO and paragraphs 4.10.9 and 4.10.11 of the AML Guideline.
[12] A financial institution as defined in the AMLO, or an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction, which has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO and is supervised for compliance with those requirements.
[13] Paragraph 3.2 of the AML Guideline.
[14] The special requirements when a customer is not physically present for identification purposes under section 9 of Schedule 2 to the AMLO and when the customer is a PEP under section 10 of Schedule 2 to the AMLO, and the special requirements in other high-risk situations under section 15 of Schedule 2 to the AMLO.

(f) placing appropriate limits on the number and types of transactions which can be undertaken pending the identity verification; and

(g) ensuring that funds are not paid out to any third parties unless certain conditions are met[15].

(ii)	**Deficiencies and inadequacies in ongoing CDD**
➢	An LC required its frontline staff to conduct annual reviews of high-risk customers' profiles but did not put in place procedural and supervisory safeguards to ensure that the annual reviews were performed. As a result, the profiles of many high-risk customers had not been reviewed or updated since their accounts were opened many years ago.
➢	An LC conducted annual reviews of high-risk customers' profiles by issuing messages to remind the customers to notify the firm of any updates to the information previously provided to the firm. The LC did not take any other steps to update the profiles of some of these customers when there were significant changes in the business relationships with these customers (eg, changes in the nature, volume or size of transactions) and when it did not receive any notifications from them.

The profiles of high-risk customers (excluding those with dormant accounts) should be subject to annual reviews, and more frequently if deemed necessary by the LCs, to ensure that the CDD information remains up-to-date and relevant[16]. LCs should institute appropriate procedural and supervisory safeguards to ensure that periodic reviews are carried out in accordance with the frequency stipulated in the firms' policies and procedures. Where significant changes in the basis of the business relationship with a customer are identified during the reviews, LCs should obtain additional relevant information to ensure that the ML/TF risks involved and the basis of the relationship are fully understood[17].

[15] Paragraph 4.7.6 of the AML Guideline.
[16] Paragraph 4.7.13 of the AML Guideline.
[17] Paragraphs 5.4 to 5.5 of the AML Guideline.

(D) Sanctions screening systems and mechanisms

Inadequacies
➢ An LC failed to incorporate some relevant sanctions designations into its internal database maintained for screening customers due to an omission by the responsible staff. ➢ Some LCs failed to implement procedures for ongoing sanctions screening against new or updated terrorists and sanctions designations after the establishment of business relationships. ➢ Some LCs failed to maintain proper documentation or records of sanctions screening results or justifications for disposing of possible name matches identified during the screening process.

LCs should implement effective sanctions screening systems and mechanisms to avoid establishing business relationships or conducting transactions with any terrorist suspects or possible designated parties.

LCs should ensure that they maintain a database (whether internal or provided by external providers) of the names and particulars of terrorists and designated parties which consolidates the various sanctions lists which have been made known to them. The database should be updated as soon as practicable whenever there are changes[18]. LCs should take appropriate measures to ensure the completeness and accuracy of the database.

LCs should screen their customers against current terrorist and sanction designations upon the establishment of the business relationship, and thereafter against any new or updated designations as soon as practicable[19]. The screening results and the justifications for disposing of potential name matches identified during the screening process should be documented or recorded electronically to demonstrate that they have been followed up and handled properly[20].

[18] Paragraphs 6.20 and 6.21 of the AML Guideline.
[19] Paragraph 6.22 of the AML Guideline.
[20] Paragraph 6.25 of the AML Guideline.

(E) Monitoring and reporting suspicious transactions

(i) Inadequacies in suspicious transaction monitoring
➢ During periodic reviews of customer accounts, some LCs failed to identify and make follow-up enquiries about securities transactions or large fund deposits made by customers which were not commensurate with the customers' profiles. ➢ Failure to identify customer transactions which exhibited red flags indicating potentially suspicious transactions for further examination: ▪ some LCs failed to make enquiries to understand the background and purpose, and assess the reasonableness, of customers' requests to make share transfers to or receive share transfers from unrelated third parties for off-exchange transactions in listed company shares by bought and sold notes which were apparently not transacted on competitive terms[21]. ▪ an LC failed to identify and assess whether there were grounds for suspicion of ML/TF in relation to an individual customer who conducted extensive trading of a single stock in two corporate accounts with the LC, both of which were beneficially owned by the customer[22]. ➢ Inadequate monitoring of potentially suspicious transactions involving direct cash deposits[23] made by customers: ▪ an LC failed to identify suspicious patterns of frequent direct cash deposits made by customers into the firm's bank account for further examination as the exception reports used by the firm for identifying potentially suspicious transactions were calibrated to capture only single cash deposits which exceeded a specific monetary threshold. The cash deposits in question appeared to have been structured to stay below the threshold. ▪ an LC relied on its junior staff to identify potentially suspicious transactions involving direct cash deposits made by customers, but failed to provide sufficient guidance to its staff, resulting in inconsistencies in judging which transactions involving direct cash deposits were potentially suspicious and should be escalated to the Money Laundering Reporting Officer for further examination.

[21] This exhibits the characteristic of the trading-related suspicious indicator (c) in paragraph 7.39 of the AML Guideline, namely a customer engages in prearranged or other non-competitive trading in particular securities, futures contracts or leveraged foreign exchange contracts.
[22] This exhibits the characteristic of the customer-related suspicious indicator (d) in paragraph 7.39 of the AML Guideline, namely a customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
[23] Large or unusual settlements of transactions in cash or where a customer only deals with an LC in cash is one of the settlement, custody and transfers-related suspicious indicators in paragraph 7.39 of the AML Guideline.

- Inadequate monitoring of potentially suspicious transactions involving third-party fund deposits[24]:
  - an LC did not examine cases where a third party made deposits into multiple customer accounts which were apparently unrelated[25] for potentially suspicious transactions.

An LC has a legal obligation to continuously monitor its business relationship with a customer by, inter alia: (i) conducting appropriate scrutiny of transactions carried out for a customer to ensure that they are consistent with the firm's knowledge of the customer, the customer's business, risk profile and source of funds; and (ii) identifying transactions which are complex, unusually large, have an unusual pattern or have no apparent economic or lawful purpose, and examining the background and purpose of those transactions[26]. The findings and outcomes of these examinations as well as the rationale for decisions made should be properly documented in writing so as to demonstrate that the LC is handling unusual or suspicious activities appropriately[27].

When considering how best to monitor customer transactions and activities, an LC should take into account, inter alia, the nature of the products and services provided (which includes the means of delivery or communication) and the ML/TF risks arising from its business[28]. LCs should have regard to a comprehensive set of red flags indicating potentially suspicious transactions, including indicators specific to the securities sector and those relating to cash or third-party transactions which are provided as examples in the AML Guideline[29], for identification of transactions which should prompt further investigations.

(ii) Inadequacies in suspicious transaction reporting and post-reporting measures

- Some LCs did not implement any measures to monitor the time it took to handle staff's internal disclosures of suspicious transactions or review suspicious transaction alerts generated from the transaction monitoring system, resulting in unwarranted delays in filing suspicious transaction reports (STRs) to the Joint Financial Intelligence Unit (JFIU).
- An LC failed to re-assess the ML/TF risk of the business relationship with a customer and take appropriate risk mitigating measures even though the LC repeatedly identified suspicious transactions in the customer's account for reporting to the JFIU.

[24] See the SFC's circular dated 3 December 2013 on Suspicious Transactions Monitoring and Reporting for further guidance on the ML/TF risks associated with third-party fund transfers.
[25] This exhibits the characteristic of the suspicious indicator in paragraph 7.14(i) of the AML Guideline, namely unnecessary routing of funds or other property from or to third parties or through third-party accounts, and the settlement/custody/transfer-related suspicious indicator (g) in paragraph 7.39 of the AML Guideline, namely a customer allocates incoming third-party deposits amongst numerous accounts.
[26] Section 5(1) of Schedule 2 to the AMLO.
[27] Paragraphs 5.10 and 5.11 of the AML Guideline.
[28] Other factors as set out in Chapter 5 of the AML Guideline are the size and complexity of the LC's business, the nature of its systems and controls and its existing monitoring procedures to satisfy other business needs.
[29] Paragraphs 7.14, 7.39 and 7.40 of the AML Guideline.

When an LC knows or suspects that a property represents the proceeds of crime or terrorist property, it has a legal obligation to file an STR to the JFIU as soon as it is reasonable to do so[30]. The need to make prompt disclosure to the JFIU is especially important where a customer has instructed the LC to move funds or other property, close the account, make cash available for collection or carry out significant changes in the business relationship. Under such circumstances, consideration may be given to contact the JFIU urgently[31].

LCs should institute appropriate measures and allocate sufficient resources to ensure that internal disclosures and suspicious transaction alerts are reviewed in a timely fashion such that they file STRs (if any) to the JFIU as soon as reasonably practicable. Such measures may include prescribing in the firm's policies and procedures the timeframe for reviews of internal disclosures and suspicious transaction alerts and, where appropriate, the filing of STRs to the JFIU; using an aging report to monitor the progress of the reviews of internal disclosures and suspicious transaction alerts such that any long-outstanding cases will be escalated to senior management for appropriate action.

It is not acceptable to continue to operate a business relationship, on which an STR report has been filed to the JFIU, without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified. LCs should conduct an appropriate review of the business relationship upon the filing of a report to the JFIU. Once an LC has concerns about the operation of a customer's account or a particular business relationship, it should take appropriate action to mitigate the risks. If necessary, the matter should be escalated to the firm's senior management to determine how to mitigate any potential legal or reputational risks posed by the relationship, in line with the firm's business objectives and its capacity to mitigate the risks identified[32].

[30] Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405) and the Organized and Serious Crimes Ordinance (Cap.455) as well as sections 12 and 14 of the United Nations (Anti-Terrorism Measures) Ordinance (Cap.575) make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property.
[31] Paragraph 7.18 of the AML Guideline.
[32] Paragraphs 5.6 and 7.33 of the AML Guideline.