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

SFC
證監會

Anti-Money Laundering and Counter-Terrorist Financing Seminar

November 2015

Raymond Wong, Director
Ronald Mak, Senior Manager
Ivan Wan, Manager

Intermediaries Supervision Department, INT Division

Disclaimer and Reminder

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) and the guidelines on AML/CFT published by the SFC, it provides information of a general nature that is not based on a consideration of specific circumstances. Furthermore, it is not intended to cover all requirements that are applicable to you and your firm. Accordingly, it should not be regarded as a substitute for seeking detailed advice on any specific case from your own professional adviser.

Agenda

- AML/CFT regulatory updates
- Adopting a risk-based approach to AML/CFT measures

AML/CFT regulatory updates

Regulatory updates - national risk assessment

- **FATF recommendation 1 and FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment**
  - Several major jurisdictions have recently undertaken NRA
  - Multi-agency effort on Hong Kong's NRA
- **This is one relevant input into the LC's assessment of the nature and extent of its ML/TF risk exposure**

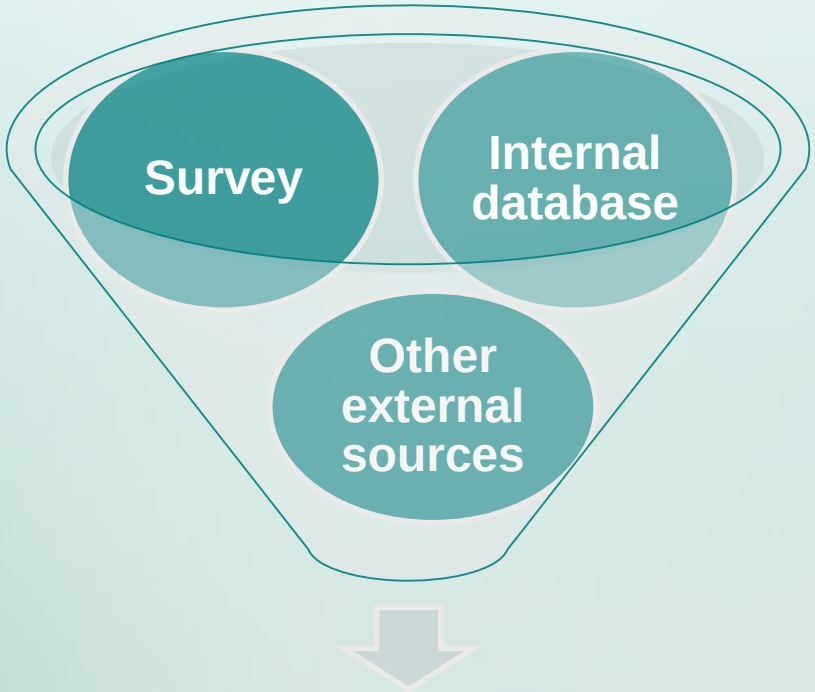
1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

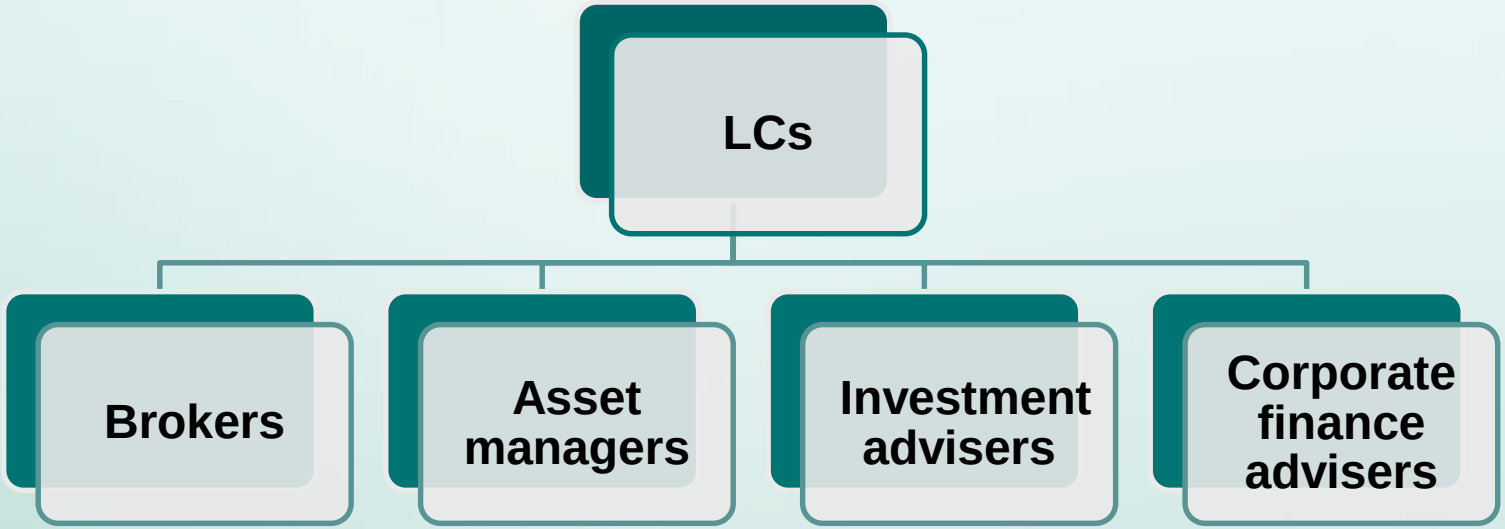
Our contribution to national risk assessment

- **Conduct risk assessment to identify, assess and understand the ML vulnerability of securities firms**
- **Draw from multiple information sources to gauge the inherent vulnerability of the sector to ML/TF and related preventive controls in place**



Securities sector assessment would form part of the national risk assessment

Money laundering risk assessment survey



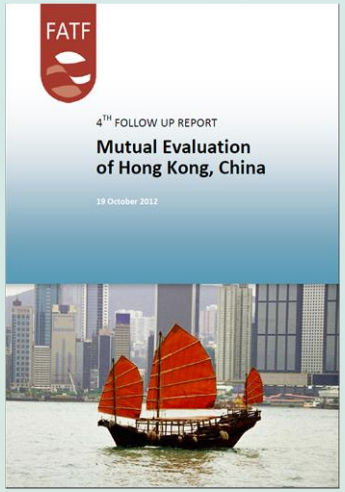
- **Business profile and AML control information obtained from a stratified sample of LCs in four main business types**

Securities sector assessment

- **This also provides an additional, useful risk identification tool to us in applying a risk-based approach to AML/CFT supervision**

FATF mutual evaluation

- **New round of Mutual Evaluation on Hong Kong, tentatively in early 2018**
- **Assesses technical compliance as well as effectiveness**
- **National risk assessment is an important prerequisite for an effective AML/CFT system at the jurisdictional level, as well as for effective (risk-based) supervision by regulators of their regulated firms for compliance with AML/CFT requirements**

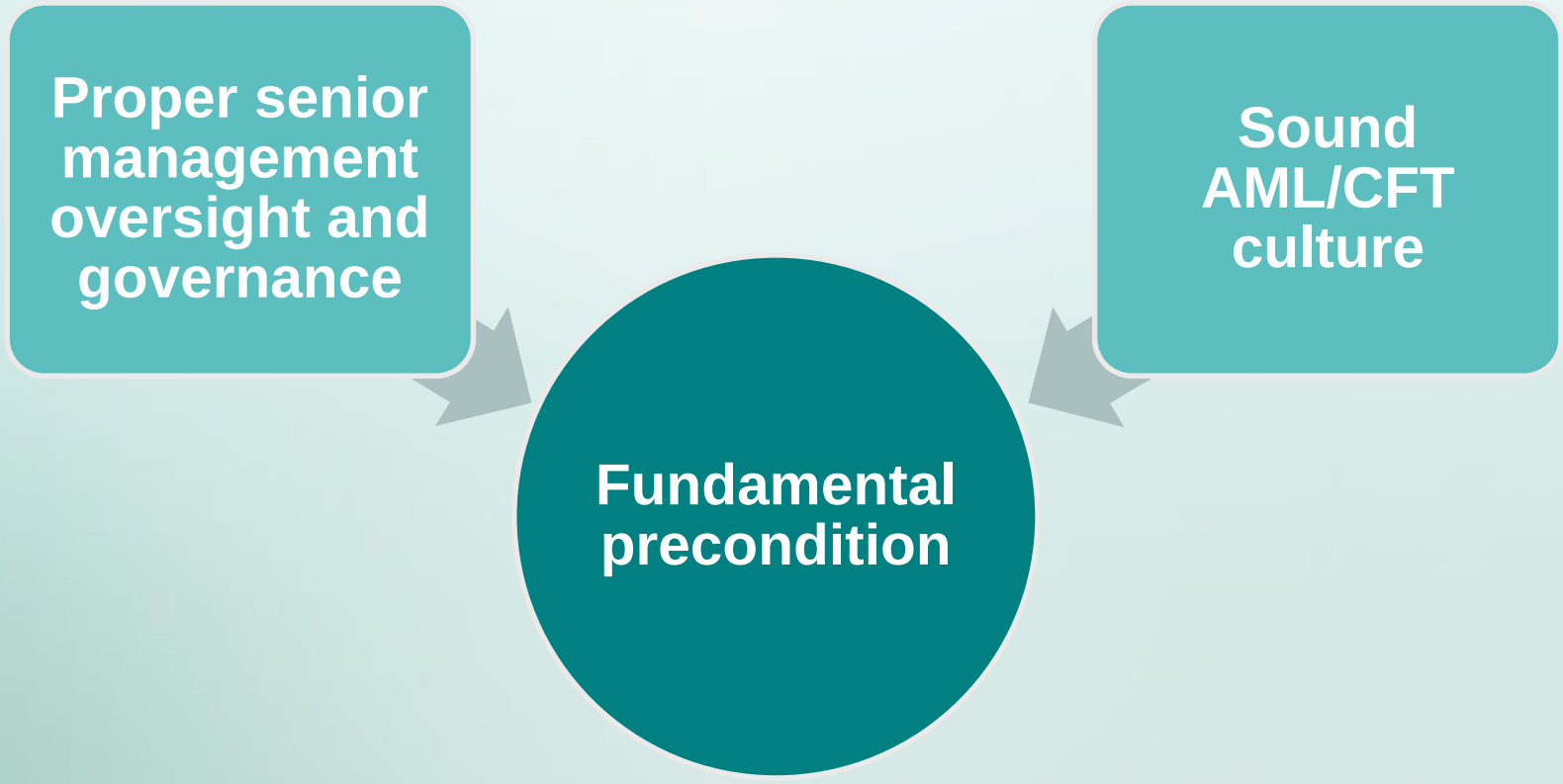


Regulatory updates - AML/CFT inspections

- **Continue to cover the full range of LCs, to monitor their compliance with AML/CFT requirements**
- **Inspections are risk based: frequency and depth of the inspection review depend on the assessed risk level of the LCs**
- **Sanctions against serious AML/CFT breaches and related internal control failures were and will be taken by the SFC**
- **Actions against culpable management personnel are also pursued**
- **In our presentation below, we will cover some of the AML/CFT good practices as well as weaknesses observed in the recent inspections**

Adopting a risk-based approach to AML/CFT measures

Adopting a risk-based approach to AML/CFT measures – fundamental precondition



Senior management oversight and governance

- A regime of senior management oversight and governance is a key component of AML compliance
- Senior management bears primary responsibility
- Senior management should know about the ML/TF risks to which the firm is exposed and be satisfied that its AML/CFT control systems are capable of addressing those risks
- Appropriate use of committee structures and/or working groups
- Clear designation and empowerment of the AML Compliance Officer and Money Laundering Reporting Officer
- Direct line of reporting from compliance and audit functions to senior management
- Role of approval for establishing or continuing business relationships with high risk customers

Governance and culture

- **Tone from the top**
- **Commit sufficient staff and technology resources**
- **Clear division of labour and accountability of staff in their particular roles in the firm with respect to AML/CFT**
- **Information sharing across the firm and appropriate reporting and escalation channels to senior management**
- **General and role specific AML/CFT training**

Adopting a risk-based approach to AML/CFT measures – some key aspects

- Institutional risk assessment
- Customer risk assessment
- Customer due diligence, including enhanced measures for higher risk customers
- Risk-based transaction monitoring procedure / system

Symbols used below:-

✓ : good practice or regulatory requirement

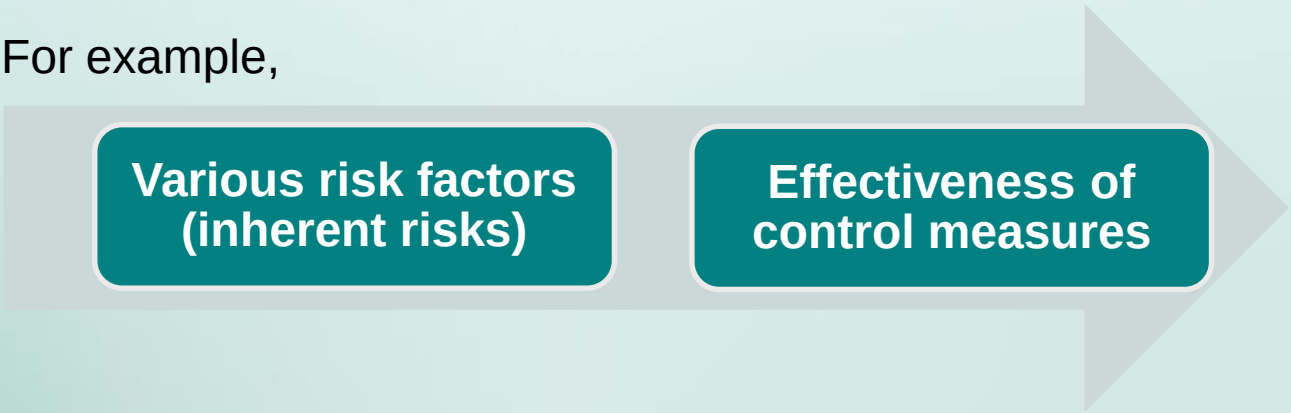
✗ : weakness or non-compliance

Institutional risk assessment

Institutional risk assessment

- **Form the basis for the RBA approach on CDD and ongoing measures**
- **Tailored assessment using proportionate processes which are commensurate with the firm's business size and complexity of operations**

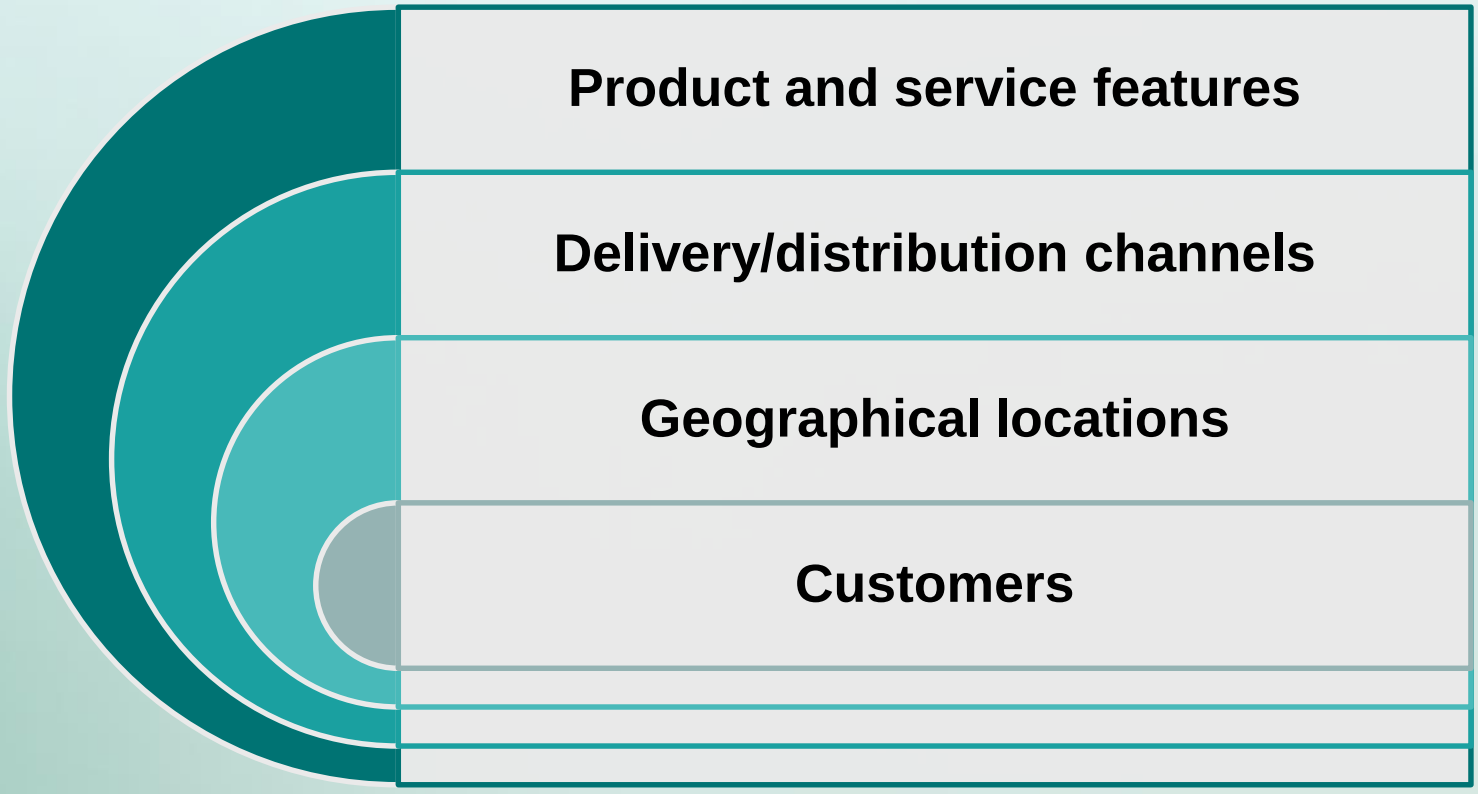
✓ For example,



Institutional risk assessment

- **Document the assessment results with sufficient details**

  ✓Sufficient qualitative assessment supported by quantitative data on business and transactions on



Institutional risk assessment

- **Examples of factors attributed to product/service risk:**
  - Products/services offered
  - Transactions with increased risk attributes
    - **Significant/unusual cash deposits and withdrawals**
    - **Transfer of fund via cross-border remittances to/from high risk countries**
    - **Significant/unusual payments/receipts to/from third parties**
    - **Accounts that are suddenly active**
  - Expected revenue growth
  - Recent/planned introduction of new products and/or services
  - Recent/planned acquisitions

Institutional risk assessment

- **Examples of factors attributed to delivery/distribution channel risk:**
  - Account origination via non face-to-face account opening
  - Account servicing via non face-to-face account approach
- **Examples of factors attributed to country risk:**
  - Any business operations in high risk jurisdictions
  - Customers' domicile, country of incorporation or nationality

Institutional risk assessment

- **Examples of factors attributed to customer risk:**
  - Varying risk profile of customers within respective customer types, for example,

Individuals	Corporates
Retail individuals vs. high net worth individuals	Privately held corporates vs. publicly held corporates vs. financial institutions

  - Special categories of customers with heightened risk attributes, e.g. customers are
    - From high risk industries
    - PEPs
  - Length of customer relationship
  - Expected customer growth

Institutional risk assessment

- **Communicate the risk assessment results with senior management**

  ✓ Senior management (Board of Director and/or relevant AML Committee) acknowledgement and/or approval of the institutional risk assessment results

  ✓ Implementation of commensurate AML measures to address the ML/TF risks identified

- **Refresh the risk assessment**

  ✓ The risk assessment is conducted on an appropriate interval or upon changes of business operations

Institutional risk assessment

- **Senior management in considering whether the LC's AML/CFT systems are capable of addressing the ML/TF risks identified should take into account, among others, the following matters:**

AML/CFT corporate governance
Sufficient management information and/or reporting
Comprehensiveness of policies and procedures
Independent review, compliance testing and oversight of AML/CFT systems and controls
Adequacy of staff training
Robust polices and procedures for recognizing and evaluating suspicious transactions for reporting to JFIU

Customer risk assessment

Customer risk assessment

- **Develop a robust customer risk assessment**
  - ✓ Take into account a broad range of high risk factors
  - – Define high risk industries, e.g.
    - Cash intensive businesses
      - – casinos and other gambling related businesses
    - Dealers in high value or precious goods
      - – art and antique dealers and auction houses
      - – dealers in precious metals, stones or jewels
    - Unregulated charities and other unregulated non-profit organizations

Customer risk assessment

- **Develop a robust customer risk assessment**
  - Determine high risk jurisdictions, e.g.
    - FATF public statements identifying jurisdictions that have strategic AML/CFT deficiencies that pose a risk to the international financial system, and jurisdictions that have such deficiencies for which they have developed an action plan with the FATF
    - Countries subject to sanctions, embargoes or similar measures
    - Transparency International's 'Corruption Perception Index'
    - The International Narcotics Control Strategy Report

✓ Provided detailed guidance to staff in recognizing higher risk situations and permitted manual adjustment of risk ratings upon proper justification and approval

✗ Limited factors were considered

✗ Failure to assign commensurate weightings to certain risk criteria to calibrate higher ML/TF risk situations

Customer risk assessment

- **Assess at the onset of business relationship and ongoing basis**

  ✓ Obtain the approval of senior management to commence or continue relationship with high risk customers as appropriate

  ✓ Refresh the risk assessment upon trigger events or periodic review of CDD profiles

  ✗ The risk assessment was never refreshed

Customer due diligence, including enhanced measures for higher risk customers

Customer due diligence

- **Application of AML/CFT requirements**
  - **Para 4.1.4a of the AML Guideline applies the "client" definition of the SFO**
  - **When an LC provides regulated services to a customer, the customer is subject to the AML/CFT requirements**
- **Adequate policies and procedures**
  - ✓ Conduct gap analysis

Customer due diligence

- **Implementation of sufficient controls to ensure adherence to policies and procedures**

  ✗ Insufficient guidance on the requisite CDD information and documents

  ✓ Supervisory review of key functions to ensure due performance (including name screening for PEPs and sanction designations)

  ✓ Complete and sign off a checklist for account opening and other key functions

  ✓ Maintain sufficient documentation to support the approval of customers, and to facilitate subsequent review

  ✓ Compliance testing on a sample basis to ensure requisite CDD information and documents are obtained, and other key functions are duly performed

Information on wealth and origin of assets

- **Gather information on wealth and origin of assets from appropriate sources to supplement declarations from the customers**

✓ Gather information on how the customers acquired wealth generally, e.g.

Search public profile from internet (e.g. Forbes.com)

Search of companies registry

Search of land records

✓ Obtain evidence to validate the origin of assets, e.g.

Bank statements of the customers

Audited accounts of the customers' business

Tax returns

Screening for PEPs

- **Establish and implement effective procedures to identify PEPs**

  ✓ The name screening covers all connected parties, and further assessment would be conducted on the customers when their connected parties are identified to be PEP

  ✓ The name screening, where applicable, covers different languages, e.g. both Chinese and English names

  ✓ The name screening will be re-performed on a periodic basis or upon trigger events

  ✗ The effectiveness of name screening could be undermined when exact match of names was applied

  ✓ Maintain sufficient documentation for subsequent review on the search results and the evaluation results on whether a name match is considered to show the customer to be a PEP

Screening for terrorist suspects and sanction designations

- **Establish and implement procedures to identify terrorist suspects and sanction designations**

  ✓ Maintain and update below lists in electronic format, e.g. Excel or Access format, to conduct screening electronically

  (i) names of terrorist suspects and sanction designations

  (ii) names of customers and all connected parties

  ✓ Maintain sufficient documentation for subsequent review on the screening performed and the evaluation results on whether a name match is considered to show the customer to be a designated terrorist or sanctioned party

  ✗ Only performed screening of a customer upon establishment of relationship but failed to perform screening of the customer again when new designations were published

  ✗ Only performed screening of customers but not payees of the customers' third party payment instructions

Use of name screening system

- **Establish and implement effective name screening procedures**

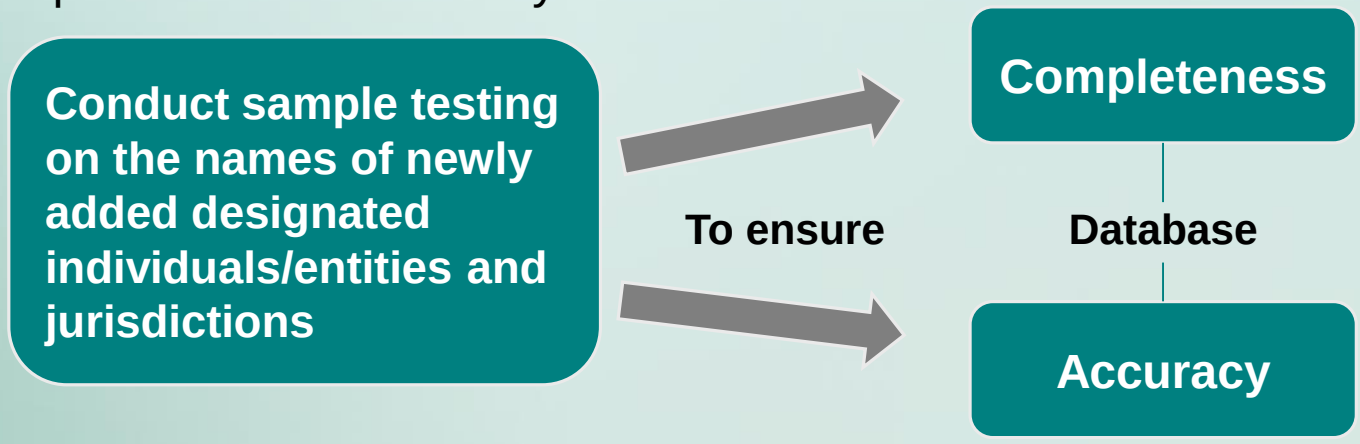
✓ Ability of the name screening system to identify names with minor alteration, such as:

Reverse order

Partial name

Abbreviated form

✓ Conduct sample testing on the database to ensure its completeness and accuracy



Keeping customer information up-to-date and relevant

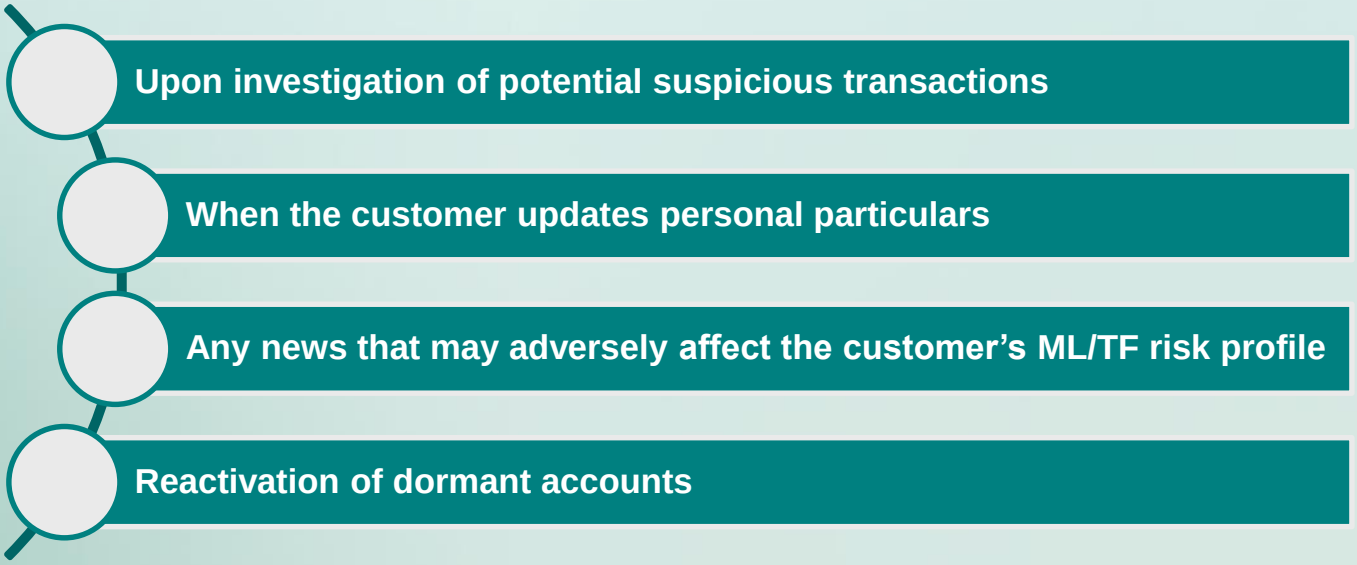
- **Review CDD profiles on a periodic basis**

  ✓ Periodic CDD review on all customers on a risk-sensitive basis

  ✓ CDD review via a mix of positive and negative confirmation and review of publicly available information

- **Review CDD profiles upon trigger events**

  ✓ Trigger events are properly defined and monitored, e.g.



CDD measures on bearer shares

- **Obtain annual declaration from customer or obtain confirmation from custodian on a periodic basis**

  ✓ Bearer share corporations are classified as high risk customers

  ✓ Only accept bearer share customers whose shares are deposited with an authorized/registered custodian and with senior management approval

  ✗ Failed to implement measures to obtain declaration from beneficial owners thereafter on an annual basis

Non-face to face account opening process

Firms are responsible for conducting proper KYC and account opening procedures

Firms should have effective policies and procedures where certifying persons are appointed

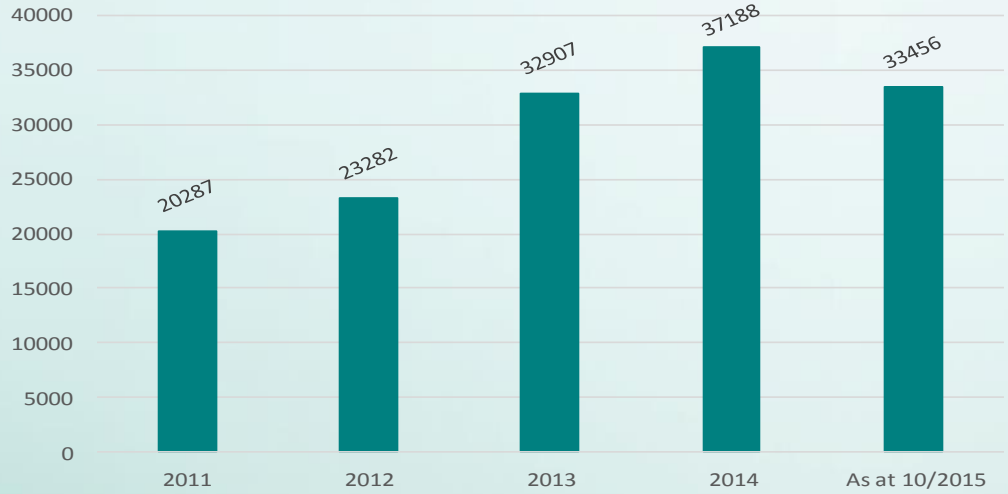
Affiliates which are not regulated financial institutions may not possess the necessary knowledge and experience

Accuracy of client information

Risk-based transaction monitoring procedure / system

STRs filed with the JFIU

- **Number of reports filed with the JFIU**



	2011	2012	2013	2014	As at 10/2015
Number of STRs per year	20,287	23,282	32,907	37,188	33,456
% of STRs filed by LCs per year	2.3%	3.0%	4.3%	4.2%	3.0%

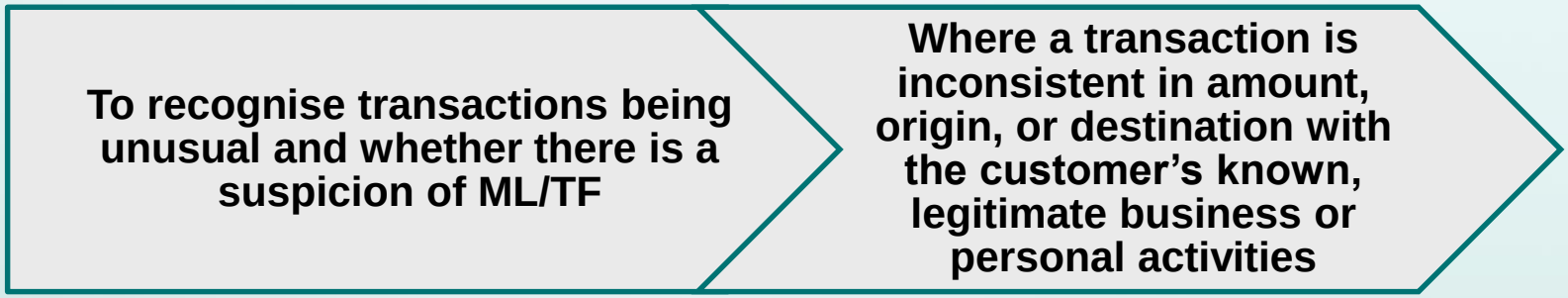
The percentage of STRs filed by LCs remains low relative to some other financial sectors, and has decreased in the first 10 months of 2015

✗ Some firms' transaction monitoring systems might not be effective in identifying all potential suspicious transactions, and firms should avoid pitfalls in the below case studies

At the same time, firms should continue to enhance their evaluation process for better quality STR reporting to the JFIU irrespective of whether this results in a larger or smaller number of reports

Effective transaction monitoring system

- **A joint effort of ALL staff and MLRO**



- **Guidance should be provided to ALL staff (front, middle and back-office) to identify suspicious transactions**

  ✗ Solely relied on its staff's manual review on their own to identify suspicious transactions for reporting (rather, MLRO should play an active role)

  ✓ A list of red flag indicators provided in the policies and procedures and properly illustrated in the training/staff meeting

  ✓ Implement a clear reporting procedure to guide staff to make internal disclosures, e.g. how and to whom he should report

Effective transaction monitoring system

- **Money Laundering Reporting Officer should play an active role**

  ✗ The MLRO acted as a passive recipient to receive internal disclosures from all staff

  ✓ Responsible personnel have good understanding on the parameters used

  ✓ Parameters are reviewed on a regular basis, e.g.

  - Investigations into suspicious activities from referrals that were not picked up by LC's system to determine the reason for this
  - Investigations on reasons why NIL alert was generated

Examples of parameters monitored by the MLRO

Changes in patterns of transactions through comparing customers' monthly transaction amount in few consecutive months

Cash receipts and transactions involving third party fund deposits and withdrawals

Trading of a particular stock frequently and earning huge profits in a short period of time, particularly before or after any corporate announcement

A customer buys and sells some low-liquidity stocks very frequently and makes a considerable loss

Frequent fund deposits and withdrawals to a securities account that is rarely used or is not being used to trade in securities

Case studies

- **List of red flag indicators**

Account which may be used as a conduit for fund transfers

Large and unusual cash deposits by a customer into the firm's bank accounts

Unverified third party receipts & payments with unusual transactions

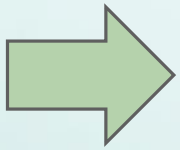
Unusual transfer of stocks to an unverified third party

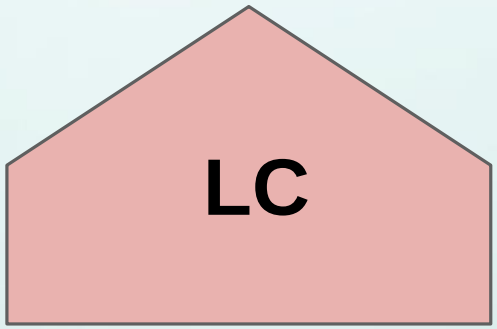
Reminder:

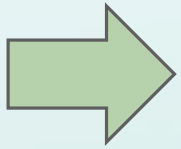
Satisfactory explanation vs. grounds for suspicion, and making a disclosure

Case study 1 - Account which may be used as a conduit for fund transfers

Remittance from Bank A







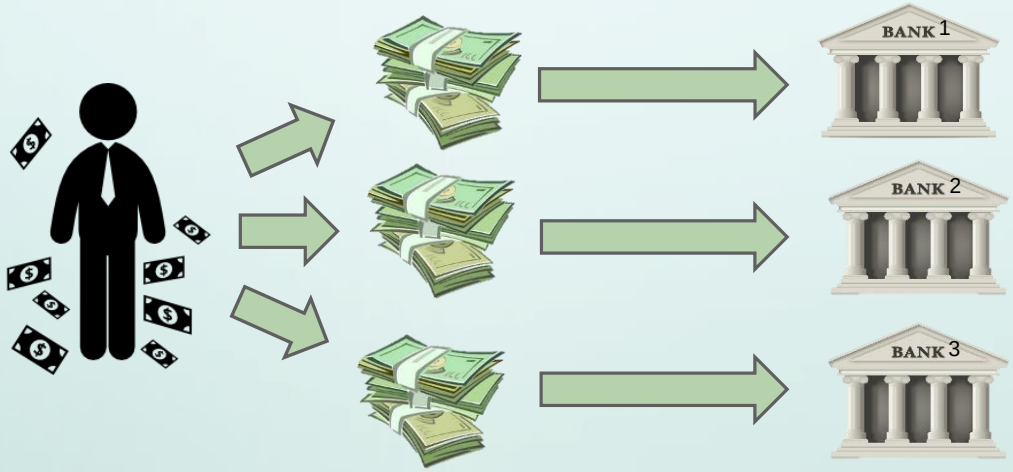
✗ Securities transactions

Remittance to Bank B

>HK$10million

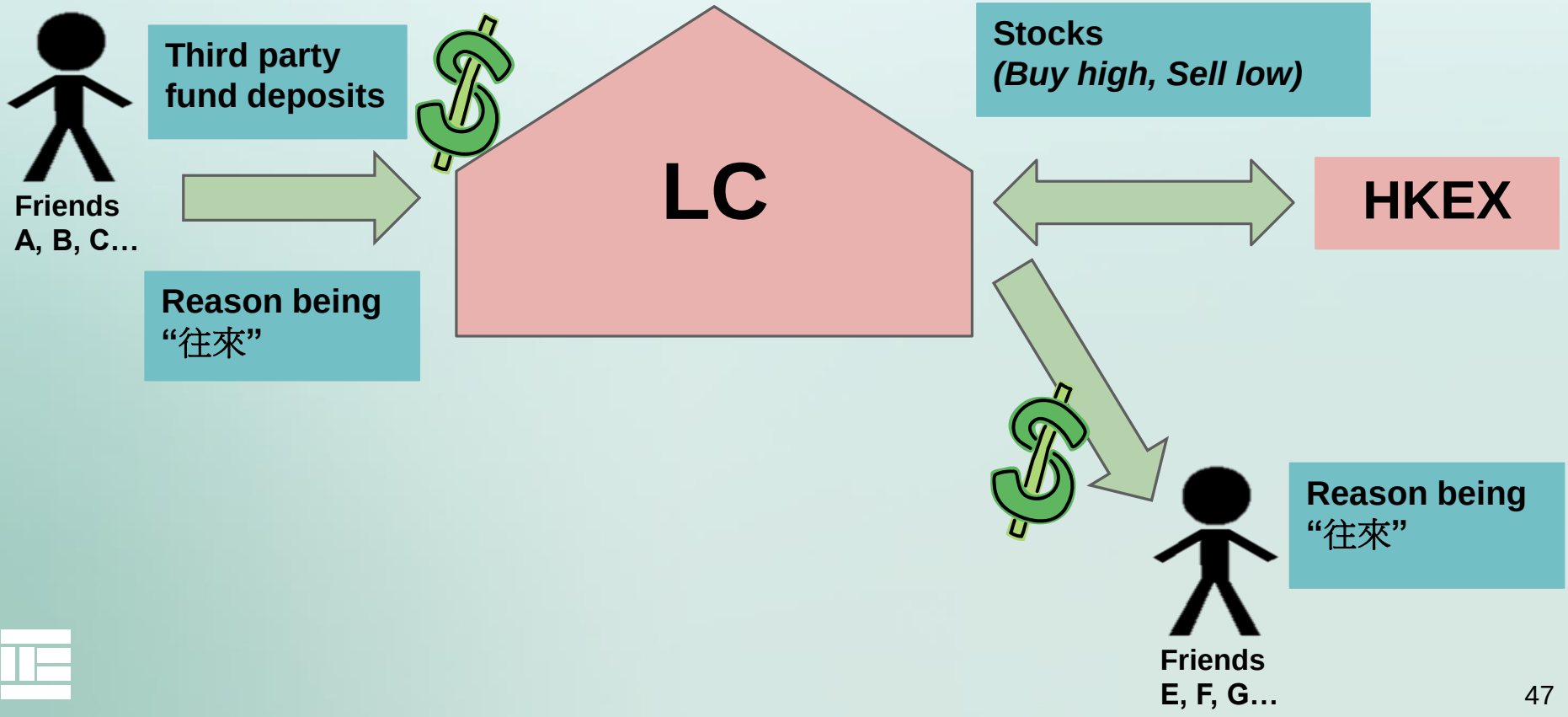
Substantially larger than declared net worth

Case Study 2 – Large and unusual cash deposits by a customer into the firm's bank accounts

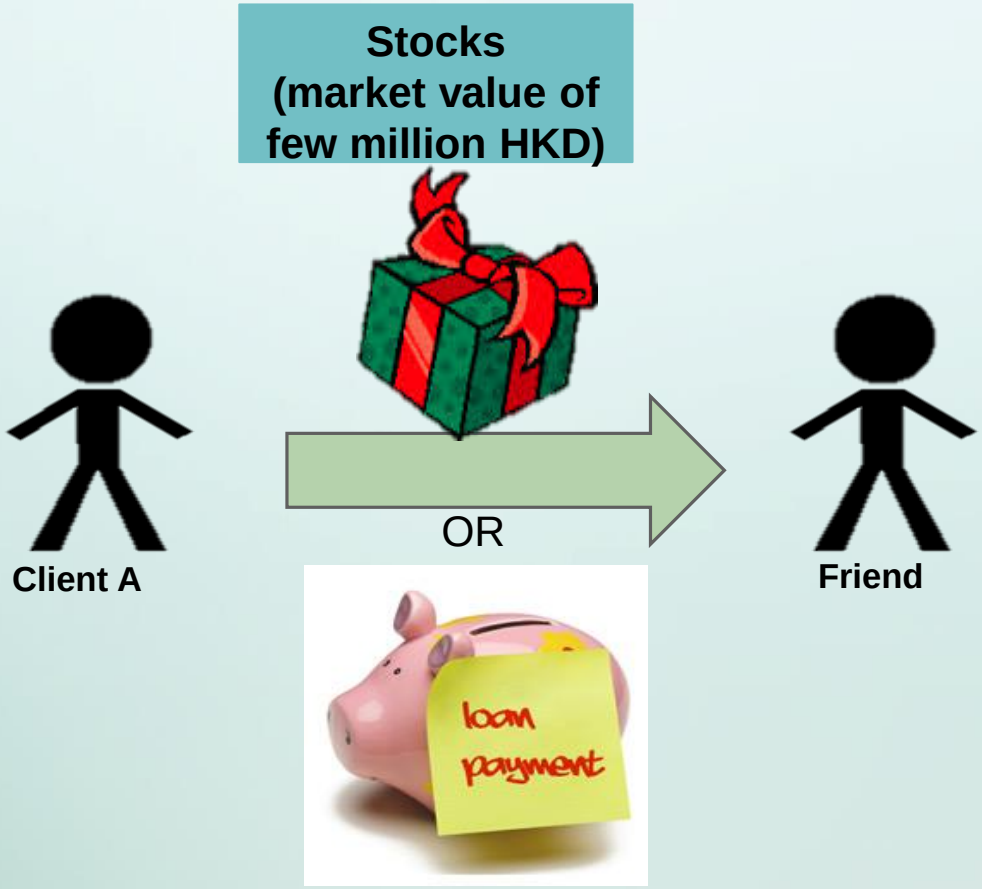


Multiple frequent cash deposits in different banks within the same day

Case Study 3 - Unverified third party receipts & payments with unusual transactions



Case Study 4 – Unusual transfer of stocks to an unverified third party



Controls over cash/third party receipts and payments

- **Implement reasonable steps to identify cash/third party receipts and payments, e.g.**

  ✓ Prohibit cash payments

  ✓ Monitor cash receipts and third party receipts via reviewing bank statements

  ✓ For deposits exceeding a monitoring threshold, obtain the customer's declaration and/or document(s) of proof, e.g. a copy of the cheque

  ✓ Keep a log sheet of cash/third party receipts and payments for MLRO's monthly review

Enhanced transaction monitoring

- **Conduct enhanced transaction monitoring for higher risk customers, e.g.**

  ✗ Monitored all customers' transactions by applying the same set of thresholds and parameters, regardless of the customers' assigned risk ratings

  ✓ Set up more stringent thresholds for higher risk customers

  ✓ Increase the frequency of review, e.g. more frequent review of SOAs for higher risk customers vs. less frequent review

  ✓ Additional review by a more senior staff in relation to potential suspicious transactions generated by higher risk customers

Evaluation of suspicious transactions

- **Implementation of adequate procedures to evaluate suspicious transactions, e.g.**

- ✓ Take into account relevant CDD information and transaction details (e.g. customer background, transaction pattern) and other supporting documents
- ✓ Consider the need for updating CDD files and conducting EDD measures
- ✓ Ensure sufficient documentation to evidence the analysis and determination of whether or not the transaction identified by an alert is suspicious
- ✓ Ensure that all alerts are reviewed in a timely manner
- ✓ Quality assurance check on a sample basis on the alert clearance documentation

Post-STR measures

- **Implement appropriate post-STR measures to mitigate ML/TF risks, e.g.**

  ✓ Restrict account activities

  ✓ Create a ‘Media Watchlist’ case to monitor negative news of customers, e.g. Factiva and/or Google alerts

  ✓ Escalation to senior management to determine whether to continue/terminate the business relationship

  ✓ Set up more stringent transaction monitoring parameters/increase the frequency of review on the accounts

Thank you