



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

Hong Kong's Money Laundering and Terrorist Financing (“ML/TF”) Risk Assessment Report

June 2018

**Raymond Wong, Director
Ivan Wan, Senior Manager
Sharon Wong, Manager**

**Intermediaries Supervision Department
Intermediaries Division**

Disclaimer and Reminder

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) and the guidelines on AML/CFT published by the Securities and Futures Commission (“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.

The SFC is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. These materials may be used for personal viewing purposes or for use within your firm. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC’s prior written consent.



Agenda

- I. Overview of Hong Kong's ML/TF risk assessment
- II. Threats and vulnerabilities
- III. How the industry may use the assessment results



I. Overview of Hong Kong's ML/TF risk assessment

A. Risk assessment results at a glance

B. The risk assessment process



A. Risk assessment results at a glance



Hong Kong ML/TF Risk Assessment

- **Hong Kong ML/TF Risk Assessment (“HKRA”) Report was published in April 2018**
- **The scope of the HKRA includes:**
 - the overall ML/TF combating ability
 - threat analysis on ML crimes
 - sectoral ML risk analysis which covers:
 - five financial sub-sectors (e.g. banking, insurance, securities, etc.)
 - five non-financial sectors (e.g. lawyers, accountants, trust or company service providers, etc.)
 - two other payment methods (i.e. store-valued facilities and virtual currencies)
 - legal persons and arrangements
 - terrorist financing



Hong Kong ML/TF Risk Assessment

– Overall ML risk

- The overall ML risk of Hong Kong:

	Threats	Vulnerabilities	Overall risk
Money Laundering	Medium-high	Medium	Medium-high

ML Threats

- **Characteristics that might heighten the ML threats of Hong Kong include:**
 - international finance, trade and transport hub
 - high degree of free trade
 - efficient financial and banking systems
 - efficient and open business environment

Hong Kong ML/TF Risk Assessment

– Overall ML risk (cont'd)

ML vulnerabilities

- Legislative and other measures have been taken to address the followings which might heighten the ML vulnerabilities of Hong Kong:
 - significant increase in the number of suspicious transaction reports (“STRs”) received by the Joint Financial Intelligence Unit (“JFIU”) presenting challenges to the JFIU in terms of handling capacity
 - gaps identified in anti-money laundering / counter-terrorist financing (“AML/CFT”) legislation *vis-à-vis* the FATF recommendations: no statutory requirements for designated non-financial businesses and professions (“DNFBPs”); transparency and beneficial ownership of legal persons; and cash couriers

Hong Kong ML/TF Risk Assessment

– *Ability to combat ML*

- **Hong Kong's ability to combat ML is characterized by the followings:**
 - robust legal framework
 - high-level political commitment
 - close partnerships among government agencies, and between public and private sectors
 - fair and efficient prosecution and judicial processes
 - good external and international cooperation

Hong Kong ML/TF Risk Assessment

– Overall TF risk

- The overall TF risk of Hong Kong:

	Threats	Vulnerabilities	Overall risk
Terrorist Financing	Medium-low	Medium-low	Medium-low

TF threats

- **Threat of isolated incidents of financing extra-territorial terrorism may be greater, as characterized by:**
 - Hong Kong's advanced and open financial system
 - cultural and economic links between certain segments of the community and regions affected by terrorism

Hong Kong ML/TF Risk Assessment

– Overall TF risk (cont'd)

TF vulnerabilities

- **Legislative and other measures have been taken to address the followings:**
 - reflect the latest sanction measures imposed by the United Nations Security Council (“UNSC”) against designated persons, entities and countries
 - amend the United Nations (Anti-Terrorism Measures) Ordinance (“UNATMO”) (Cap.575) to prohibit any person from dealing with specified terrorist property and property of specified terrorists or terrorist associates, and to criminalise, among other things, the financing of travel between states for the purpose of perpetration, planning or preparation of, or participation in, terrorist acts or the provision or receiving of terrorist training

Hong Kong ML/TF Risk Assessment

– A summary of the measures taken to address the identified ML/TF risks

■ **Enhancing the AML/CFT legal framework**

- amended the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (“AMLO”) (Cap. 615), the Companies Ordinance (Cap. 622) and the UNATMO
- introduced the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629)
- implement the latest UNSC sanctions against the Democratic People’s Republic of Korea

■ **Strengthening risk-based supervision and partnerships**

- review and update the AML/CFT Guidelines to ensure that the requirements are in line with the latest international standards
- pursue ongoing supervisory effort to promote implementation of risk-based AML/CFT systems that are critical for protecting the safety and soundness of FIs and the integrity of Hong Kong’s financial system
- engage private sectors more prominently as partners in combating significant ML threat e.g. through a police-led platform for the discussion of cases, trends and typologies and the sharing of intelligence



Hong Kong ML/TF Risk Assessment

– A summary of the measures taken to address the identified ML/TF risks (cont'd)

- **Sustaining outreach and raising awareness**
 - sustain outreach to ensure adequate awareness and understanding of the ML/TF threats and the high-risk patterns
- **Monitoring new and emerging risks**
 - monitor risk and keep abreast of new and emerging typologies
- **Strengthening law enforcement efforts**
 - continue to step up ML/TF investigation, leverage the use and exchange of financial intelligence and multi-agency collaboration
 - strengthen international cooperation with overseas authorities

B. The risk assessment process



Hong Kong ML/TF Risk Assessment

– *Methodology*

- In conducting the HKRA, the Government has:
 - made reference to the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*
 - adopted the World Bank National Risk Assessment Tool (“World Bank Tool”)
- The World Bank Tool was used to help identifying the main drivers of ML/TF risks through understanding of the causal relations among risk factors and variables relating to the regulatory, institutional and economic environment

Methodology of the World Bank Tool



Threat refers to:

the scale and characteristics (or patterns) of the generation, inflows, and outflows of the proceeds of crime or funds linked with terrorism.

- **ML threats** assessment includes predicate offences that generate crime proceeds, total size of the crime proceeds, sectors in which proceeds are invested and laundered, etc.
- **TF threats** assessment includes the direction of TF funds, and the sources and channels used

Vulnerability refers to:

the weaknesses or gaps in a jurisdiction's defenses against ML/TF.

- **Vulnerabilities** assessment includes the AML/CFT legislative framework, the effectiveness of law enforcement and supervision, quality of suspicious transaction reporting, AML/CFT awareness, inherent factors such as geographic / demographic characteristics / size of economy or sector concerned, etc.

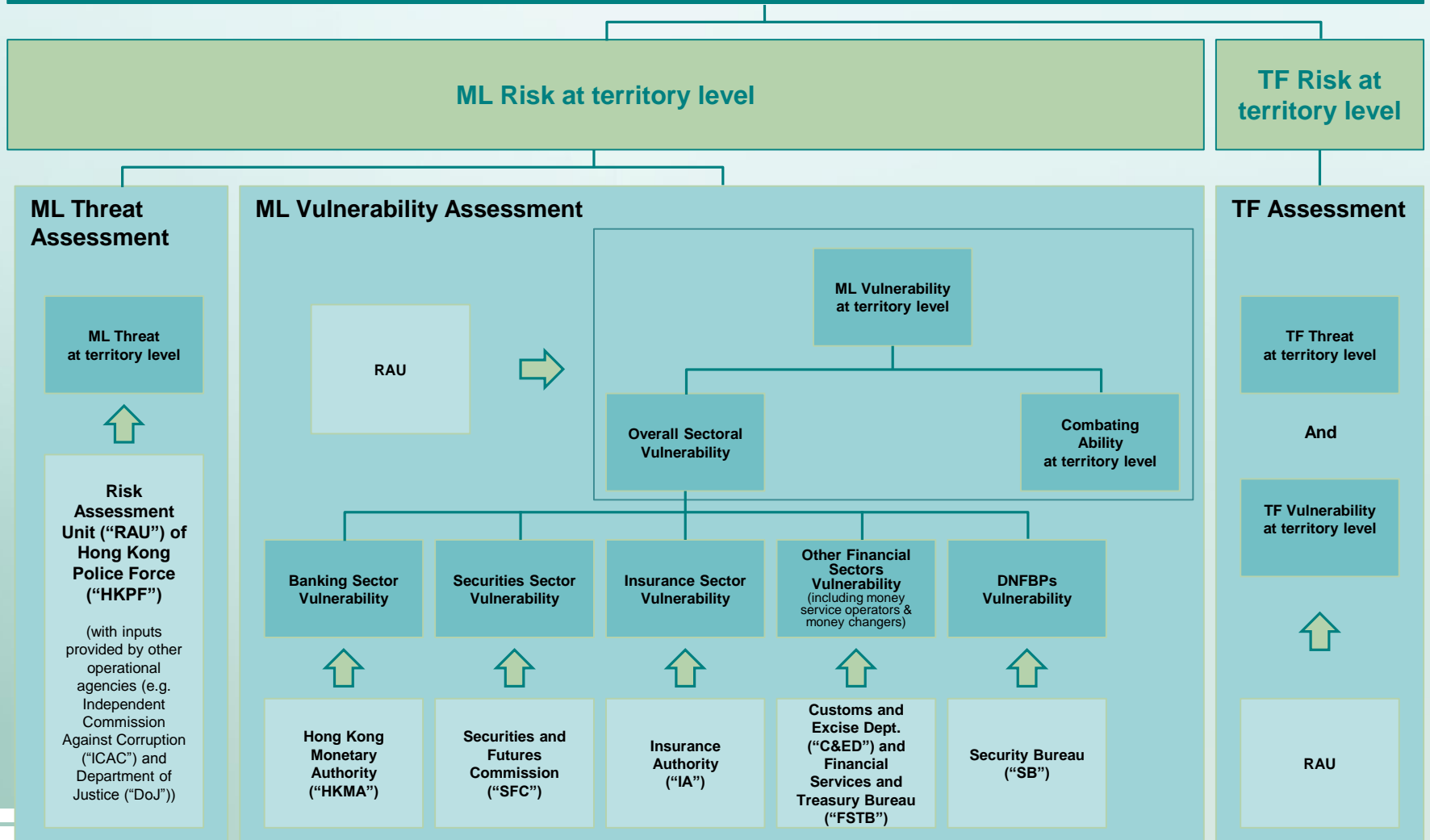
Risk is:

a combination of threats and vulnerabilities at the territory level.

- **ML risk** is a function of threats and vulnerabilities of individual sectors as well as the jurisdiction ability to combat ML activities
- **TF risk** is an outcome of TF threats and vulnerabilities

Hong Kong ML/TF risk assessment

ML and TF Risk



Hong Kong ML/TF risk assessment

– *The Steering Committee*

- A Steering Committee of the ML/TF Risk Assessment in Hong Kong was established to oversee the conduct, monitoring the progress, and evaluate the findings of the HKRA

- Led by the FSTB and direct engagement with financial regulators, law enforcement agencies, government bodies include the following:
 - the SB
 - the C&ED
 - the DoJ
 - the HKPF
 - The Commerce and Economic Development Bureau
 - the ICAC
 - the HKMA
 - the SFC
 - the IA

II. Threats and vulnerabilities

A. ML threats to the securities sector

B. ML vulnerabilities of the securities sector

C. Typologies analysis and ML trends

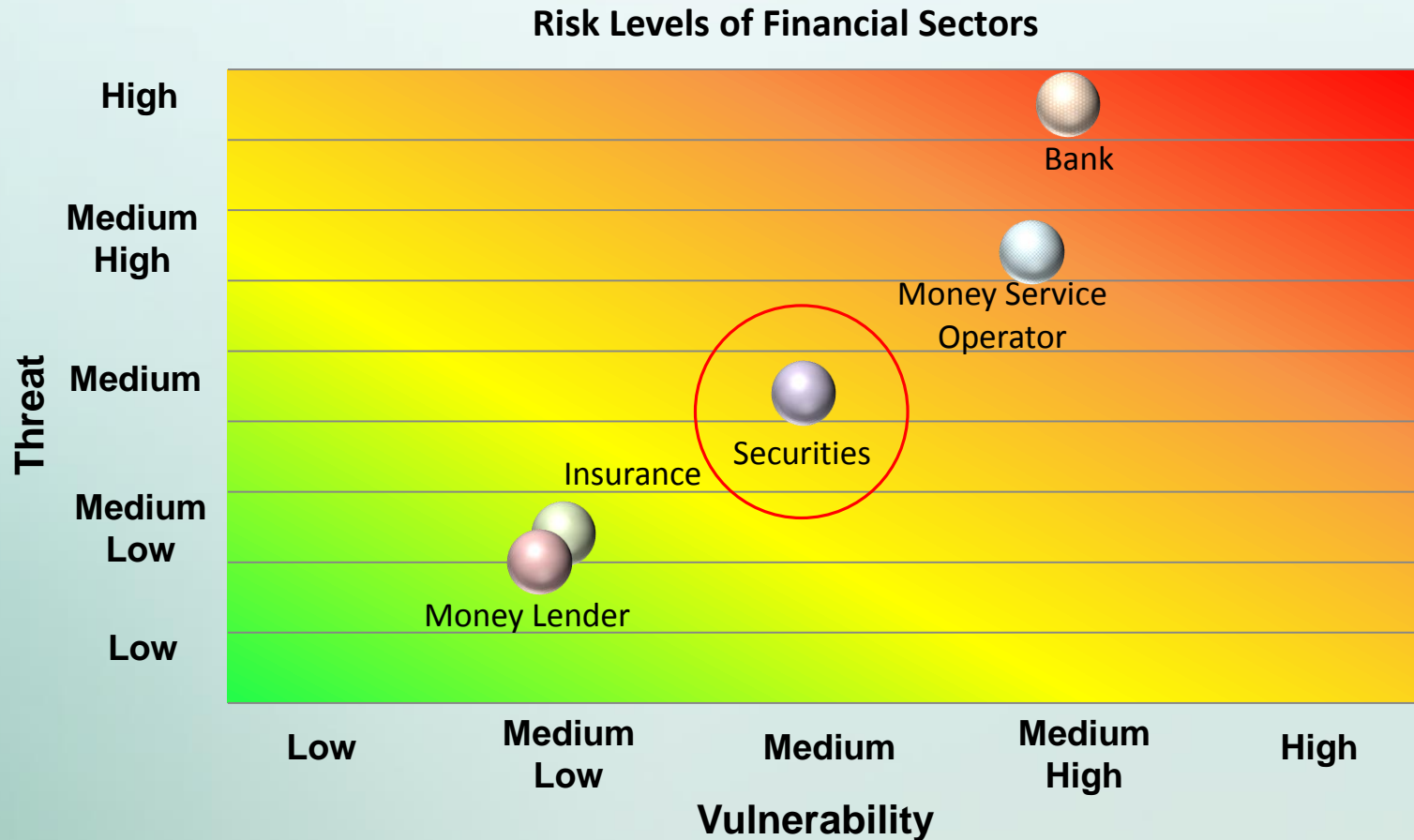
D. Threats and vulnerabilities of other payment methods

E. Threats and vulnerabilities of terrorist financing



Securities sector ML risk assessment

– *ML risk level of securities sector*



A. ML threats to the securities sector



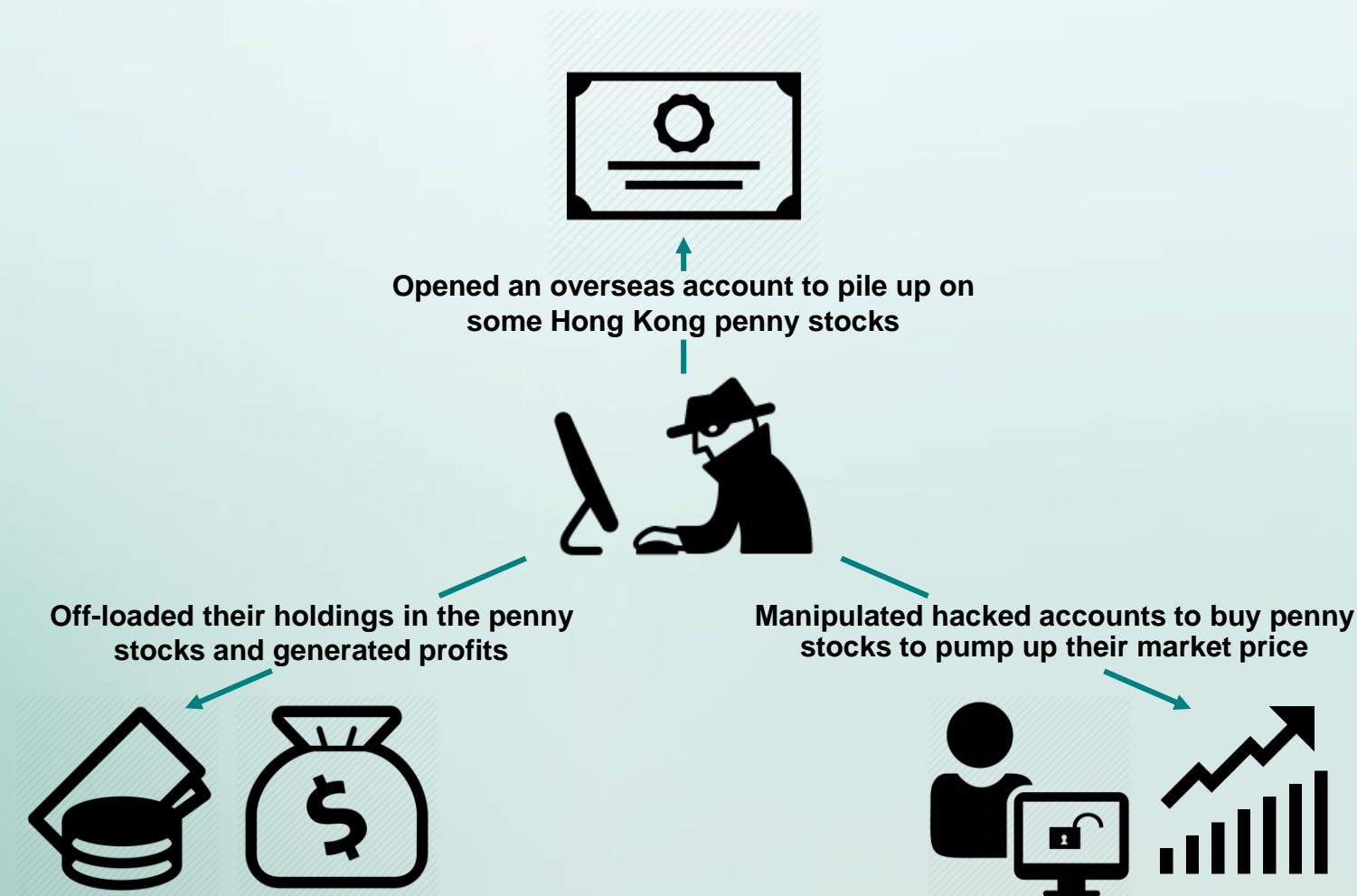
ML threats to the securities sector

- Hong Kong's securities sector is exposed to both **domestic and transnational ML threats** due to:
 - its globalized nature, and high volume of transactions and liquidity
 - the prevalence of cross-border transactions and exposure to non-Hong Kong clients who may be connected with corruption, tax evasion and other predicate offences
- The securities sector is less conducive to the **placement of illicit proceeds** as industry does not normally accept cash. It can be misused to:
 - generate illicit proceeds through securities-related predicated offences
 - launder illicit proceeds from non-securities related offences



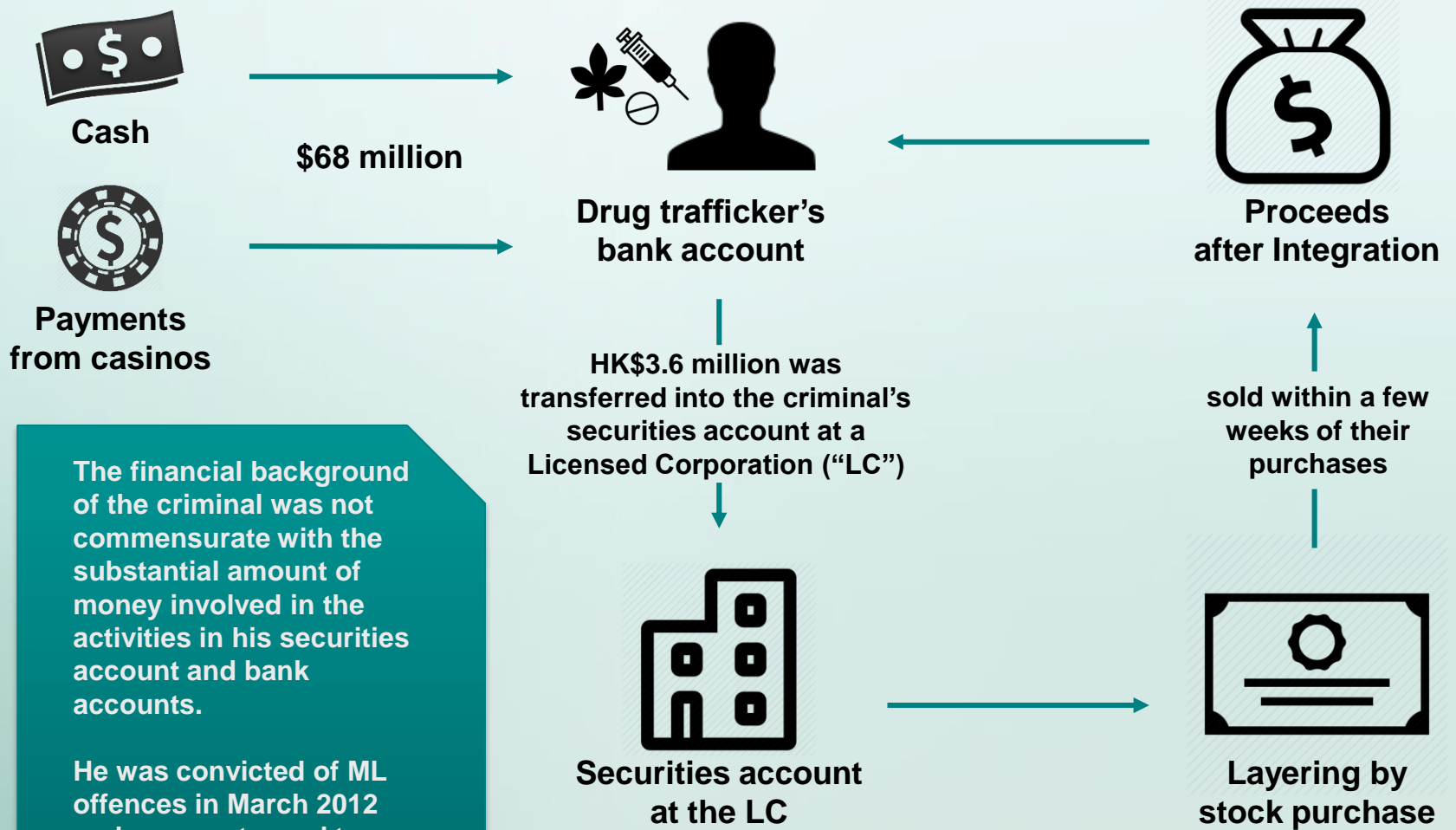
ML Threats from securities related predicated offences

Case Study – “Pump and dump” scheme



ML Threats from non-securities related predicated offences

Case study – Use of securities account to launder illicit proceeds



The financial background of the criminal was not commensurate with the substantial amount of money involved in the activities in his securities account and bank accounts.

He was convicted of ML offences in March 2012 and was sentenced to imprisonment of 5 years.

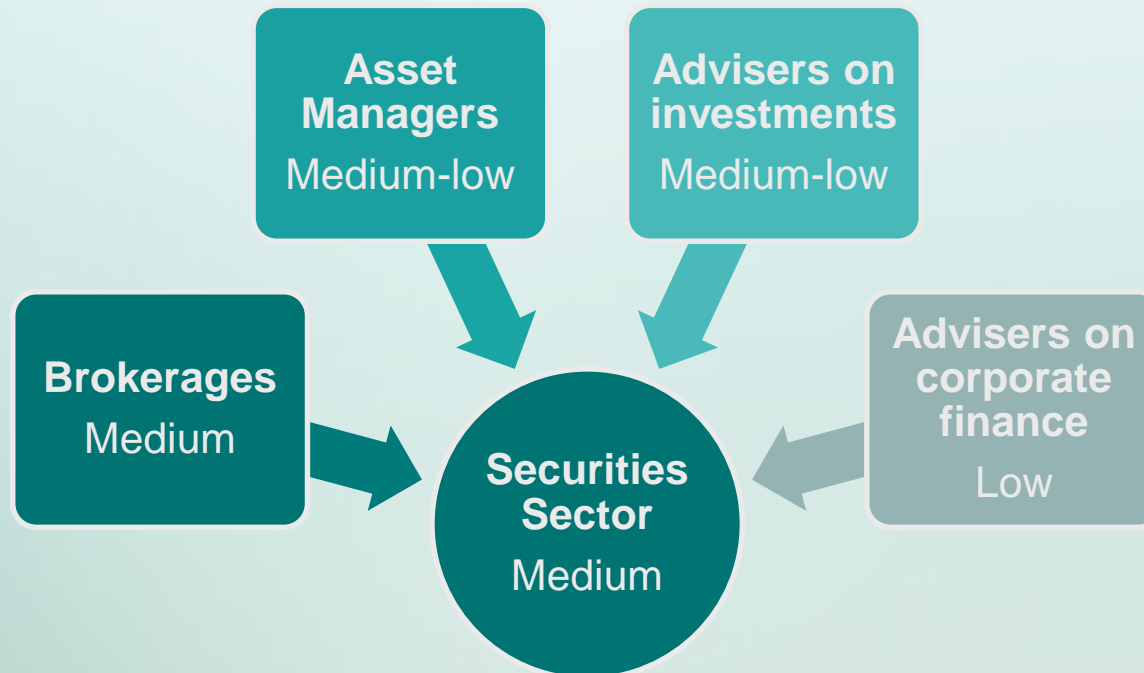


B. ML vulnerabilities of the securities sector

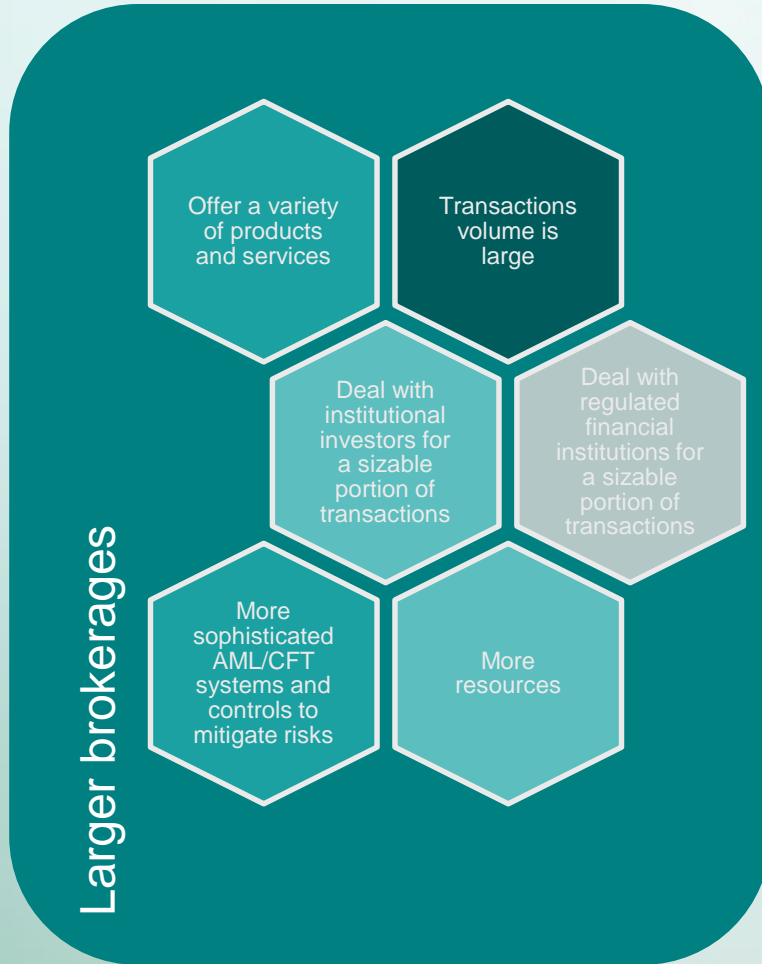


ML vulnerabilities of the securities sector

- For ML vulnerability assessment, LCs' business activities are classified into four major sub-sectors by taking into account the inherent vulnerabilities arising from specific features and users of the subsector



Key features of brokerages



ML vulnerabilities of brokerages

– *Third party receipts or payments*

■ **Factors that affect its ML vulnerabilities:**

- ▲ money launderers may receive or pay funds from or to third parties to conceal the control and ownership of their securities accounts and source of funds
- ▼ industry participants generally considered third party receipts or payments pose ML risk to their businesses. Some brokerages therefore restrict third party payments, while others that accept such payments regard them as a red-flag indicator for potentially suspicious transactions
- ▼ the SFC's Guideline on Anti-Money Laundering and Counter-Terrorist Financing includes frequent funds or other property transfers to or from third parties that are unrelated, unverified or difficult to verify among other examples of red-flag indicators
- ▼ the SFC reminds LCs to be vigilant in monitoring ML/TF risks associated with third party payments through advisory circular issued in January 2017 and industry outreach events

Legend: ▲ Factors that may increase the ML vulnerabilities
▼ Factors that may reduce the ML vulnerabilities

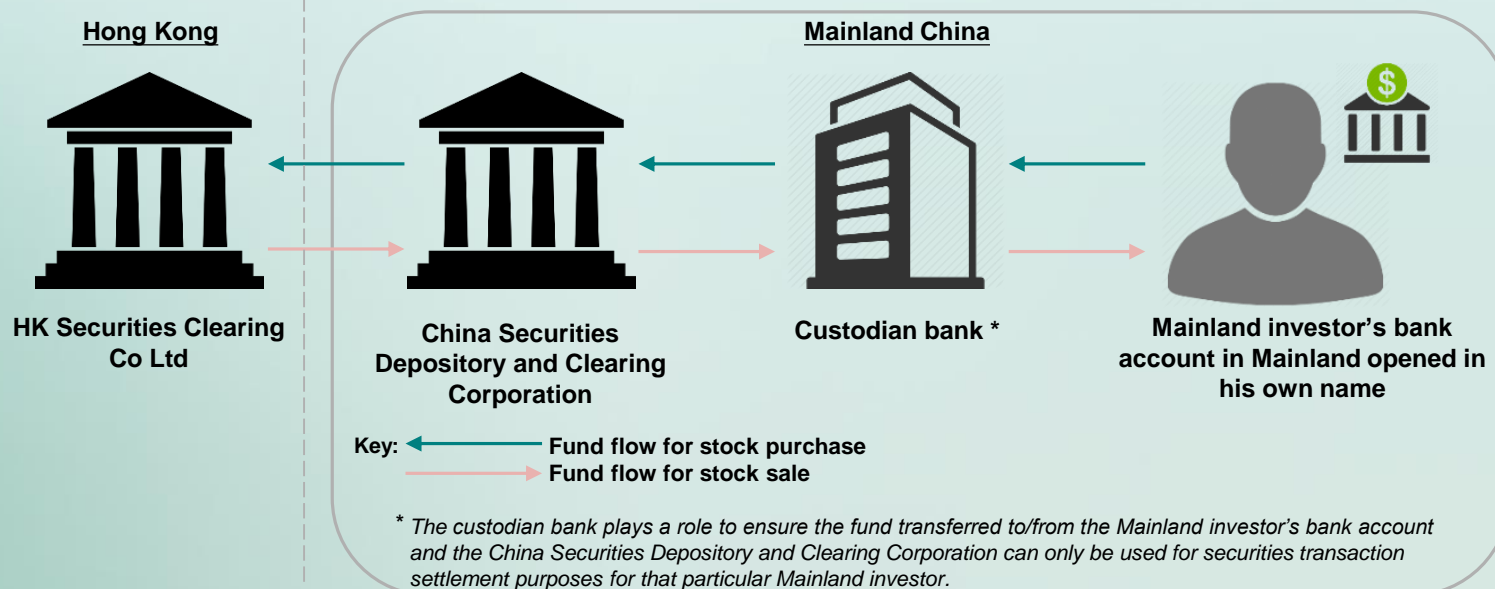


ML vulnerabilities of brokerages

– Linkage to markets outside Hong Kong

Mainland-Hong Kong Stock Connect (“Stock Connect”)

- **Factors that affect its ML vulnerabilities:**
 - ✓ eligible Mainland investors can trade Hong Kong stocks through accounts with Mainland brokerages which apply customer due diligence (“CDD”) and other measures similar to those set out in the AMLO
 - ✓ the closed-loop cross-boundary fund flow requirement of Stock Connect
 - ✓ the Memorandum of Understanding entered between the SFC and the China Securities Regulatory Commission for strengthening cross-boundary regulatory and enforcement cooperation pertaining to the Stock Connect



ML vulnerabilities of brokerages

– *Non-face-to-face account opening*

- **Factors that affect its ML vulnerabilities:**
 - ▲ non-face-to-face account opening is vulnerable to identity fraud
 - ▼ many brokerages do not accept non-face-to-face account opening
 - ▼ additional measures are generally applied by industry participants where an account opening procedure other than a face-to-face approach is used, for example:
 - use of suitable persons (e.g. a lawyer) to certify verification of identity documents
 - ▼ the SFC issued an advisory circular in 2016 to provide further guidance on client identity verification in account opening process in a non-face-to-face situation where a client is not physically present

Key features of asset managers

- Generally do not hold client assets
- Money movement typically through banks or regulated FIs
- For institutional clients and managed accounts whose sales and marketing are performed by asset managers, asset managers apply CDD and transaction monitoring on investors directly
- For SFC-authorized funds distributed to retail investors, CDD and transaction monitoring are applied normally through intermediaries



ML vulnerabilities of asset managers

– *Exposure to transnational ML*

- **Factors that affect its ML vulnerabilities:**
 - ▲ over 60% of the funding for Hong Kong's fund management business came from overseas investors
 - ▼ stringent CDD measures and transaction monitoring on investors must be conducted by the asset managers and/or service providers appointed by the funds

ML vulnerabilities of asset managers

– *Linkage to markets outside Hong Kong*

Hong Kong and Mainland Mutual Recognition of Funds

- Distribution channel of eligible SFC-authorized Hong Kong funds has been extended to the Mainland investors
- **Factors that affect its ML vulnerabilities:**
 - ▼ inherent vulnerability to cross-border ML is mitigated by the arrangement that recognized Hong Kong funds are distributed by Mainland financial institutions which are subject to similar AML/CFT regulations
 - ▼ the SFC entered into regulatory and supervisory cooperation arrangements with the China Securities Regulatory Commission



Vulnerabilities of asset managers

– *Private client funds / Discretionary account management*

- **Factors that affect its ML vulnerabilities:**
 - ▲ may be used by high-net-worth individuals to set up complex products and diversified portfolios for ML purposes in relation to tax evasion and corruption
 - ▼ private client funds under management by LCs accounted for less than 10% of the aggregate asset management and fund advisory business in Hong Kong
 - ▼ asset managers generally meet investors of discretionary account management in person to carry out CDD and monitor the investors' fund deposits/withdrawals to identify suspicious activity



Vulnerabilities of advisers on investments

- **Factors that affect its ML vulnerabilities:**
 - ▲ vulnerable to being implicated into ML schemes such as tax evasion
 - ▼ advisers on investments are normally subject to a licensing condition that they shall not hold client assets
 - ▼ mostly give advice on non-exchange traded investment products with relatively low liquidity and high transaction costs, such as structured products, fixed income products, swaps and repos, etc.

Vulnerabilities of advisers on corporate finance

- **Factors that affect its ML vulnerabilities:**
 - ▲ vulnerable to being drawn into ML at the layering and integration stages
 - ▼ advisers on corporate finance are normally subject to a licensing condition that they shall not hold client assets
 - ▼ generally perform due diligence on clients to better understand their business nature, financial circumstances and purposes of the transactions under consideration in addition to AML/CFT procedures
 - ▼ clients are mostly listed corporations or corporations planning to go public or whose owners are subject to high transparency standards

Cybersecurity

Increasing **cyber-attacks**

Within **18 months** up to 31 March 2017

Reported **27** cybersecurity incidents

Involved **12** securities brokerages

Customers' **Internet-based trading** accounts were hacked

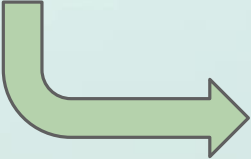
Executed **over \$110m** total unauthorized trades



Non-face-to-face account opening

Generally unable to determine the identity documents provided belong to the client

Use of new technology for client identity verification during non-face-to-face account opening



Emerging Risk



C. Typologies analysis and ML trends



Third-party money laundering

- **Use of third parties** to launder proceeds generated domestically or outside Hong Kong
- **Recruited to open bank accounts** for a small monetary reward
- **Commonly involve:**
 - non-residents
 - students
 - low-paid stooges



Money laundering involving professionals

- Professionals can be used by criminals who need expert advice to **devise complicated ML schemes**
- Cases of complicit involvement of professionals in ML in Hong Kong are **relatively rare**
- **Three cases** involving accountants convicted in 2010, 2011 and 2014
- In 2015, **16 ML cases** leading to convictions involved the use of trust or company service providers (“TCSP”) services, where many TCSPs in Hong Kong are owned or managed by **solicitors** or **accountants**



Misuse of legal persons and arrangements

- **Use of complex ownership structure, trust, shell companies, etc. to:**

- hide proceeds of corruption, tax evasion
- conceal ownerships
- dissipate drug proceeds
- transfer crime proceeds under the disguise of payments resulting from legitimate business activities



- **Corporate vehicles and legal structures are inherently attractive for ML because:**

- more reasonable to move large sums of money in appearance
- takes time and multiple efforts to verify the source of the funds or the alleged trade or business if fictitious invoices or shipping documents are used
- may hide beneficial owners or persons who control the company
- commingling of legitimate and unlawful activity makes it harder to distinguish companies' assets from crime proceeds
- criminals may take advantage of the transactions with reputable companies to minimise suspicions



Rise of technology crime

- **Elevated scale** of sophistication and penetration of technology crimes
- Criminals have taken advantage of increased online business activities, rapid movements of money, enhanced telecommunications and computer links
- In 2015, total reported loss from technology crime amounted to **HK\$1.83 billion**, of which corporate email scams accounted for **HK\$1.37 billion**



Analysis of STRs

Some common reported suspicious indicators:

Large Transaction

Large Cash Transaction

Non-resident personal account

Transaction incommensurate with customer background

Temporary repository of funds



Types of assets in restraint and confiscation order (2011-2015)

To disguise the source of money, crime proceeds may be converted into forms that are difficult to retrace:

Types of assets	Restraint order		Confiscation order	
	Amount (HK\$m)	%	Amount (HK\$m)	%
Assets placed in banks	2,085.09	55.96%	2,567.08	86.12%
Real estate	919.86	24.69%	287.06	9.64%
Securities	530.89	14.25%	6.21	0.21%
Precious metals and stones, jewellery or wristwatches	91.60	2.46%	89.28	2.99%
Cash	34.47	0.92%	20.35	0.68%
Insurance policies / products	17.93	0.48%	7.45	0.25%
Vessels	15.24	0.41%	-	-
Vehicles	14.25	0.38%	1.43	0.05%
Uncategorised company assets	10.70	0.29%	0.57	0.02%
Others	6.06	0.16%	1.12	0.04%

D. Threats and vulnerabilities of other payment methods



Other payment methods

– *Virtual currencies*

The ML risk of virtual currencies (“VCs”) is assessed as medium-low

- Anonymous and decentralized nature of some VCs pose potential ML/TF risks
- No apparent sign of organized crime or ML/TF concerning trading of VCs, but VCs have been used as a pretext in a Ponzi scheme or as payments in cybercrimes
- No visible impact affecting the overall risk in Hong Kong
- No specific regulation over virtual currencies
- The Government and financial regulators have issued warnings of consumer, ML/TF and cybercrime risks associated with VCs
- Financial regulators also issued circulars to remind regulated institutions that they should ensure vigilance when considering whether to establish or maintain relationships with operators of schemes related to VCs
- Current legal and regulatory provisions relating to ML/TF, fraud and other crimes are wide enough to catch offences involving the use of VCs



Other payment methods

– *Virtual currencies (cont'd)*

- Firms should guard against the ML/TF risks associated with potential or existing customers that are operators of schemes related to virtual commodities, by increased vigilance in assessing the ML/TF risks of customers as well as monitoring and detecting unusual or suspicious transactions

Source: SFC circulars on Money Laundering and Terrorist Financing Risks Associated with Virtual Commodities issued on 16 January 2014 and 21 March 2014

- Dealing in or advising on the digital tokens or managing or marketing a fund investing in such digital tokens may constitute a regulated activity if the digital tokens fall under the definition of securities

Source: SFC statement on initial coin offerings issued on 5 September 2017



E. Threats and vulnerabilities of terrorist financing



Terrorist financing

- **Traditional TF methods and techniques:**
 - abusive of donations and non-profit organisations
 - funding from criminal or legitimate activities
 - physical transportation of cash
 - use of bank accounts and money service operators
- **Social media platforms and new payment products and services have been exploited for TF**



Terrorist financing (cont'd)

- **Hong Kong has a medium-low TF risk**
 - STRs and investigation as well as TF-related mutual legal assistance requests have not led to confirmation of any TF activity in Hong Kong or discovery of high-risk patterns
 - available information does not indicate the use of technology (e.g. social media platforms, online payment systems, virtual currencies, etc.) being exploited for TF purposes
 - the threat of financing terrorism abroad may be greater given Hong Kong has an advanced and open financial system
 - Hong Kong has a sound legal and institutional framework to counter TF activities which is commensurate with the threat identified

Early alert system

- To complement the timely implementations of new or revised sanctions resolutions or sanctions lists
- The SFC issues alerts via its website and/or circulars whenever new or revised sanctions resolutions or sanctions lists relating to terrorism, terrorist financing and weapons of mass destruction proliferation are promulgated by the UNSC
- Firms should ensure that their screening databases are updated as soon as practicable whenever the abovementioned alerts are issued by the SFC, regardless of whether the relevant sanctions have been implemented in Hong Kong via the UNSO or otherwise

Source: SFC circular on United Nations Sanctions issued on 7 February 2018



III. How the industry may use the assessment results

A. Institutional risk assessment

B. Customer risk assessment

C. Suspicious transaction monitoring

D. Other measures



FATF Recommendations and Guidance



FATF Recommendation 1 and the interpretive note

1. Financial institutions and DNFBPs should:

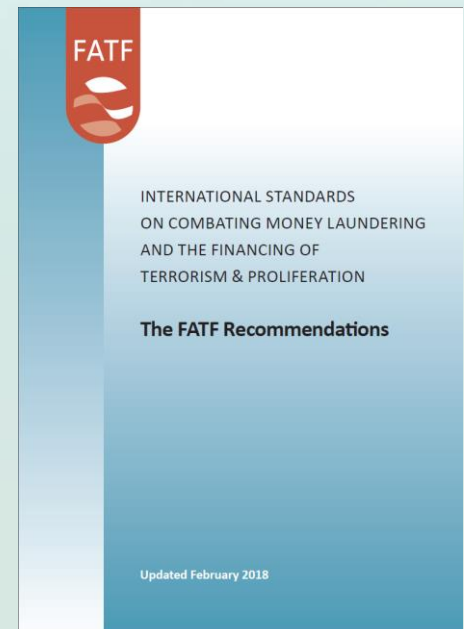
- identify and assess their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions and delivery channels)

2. Financial institutions and DNFBPs should:

- document those assessments in order to be able to demonstrate their basis, keep these assessments up-to-date, and have appropriate mechanisms to provide risk assessment information to competent authorities

■ So as to:

- understand their ML/TF risks
- have policies, controls and procedures to enable them to manage and mitigate effectively the risks identified



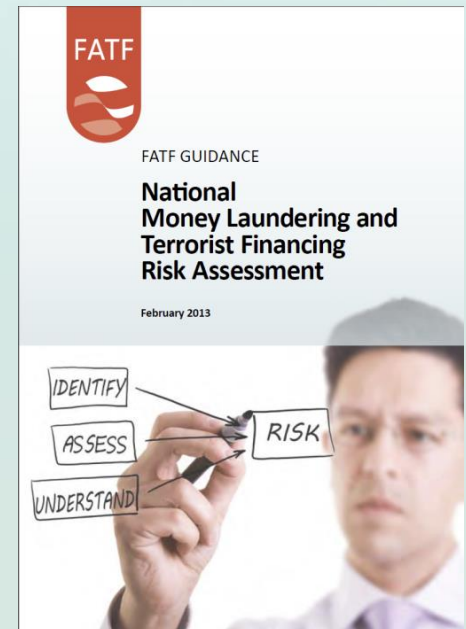
FATF Recommendations and Guidance (cont'd)



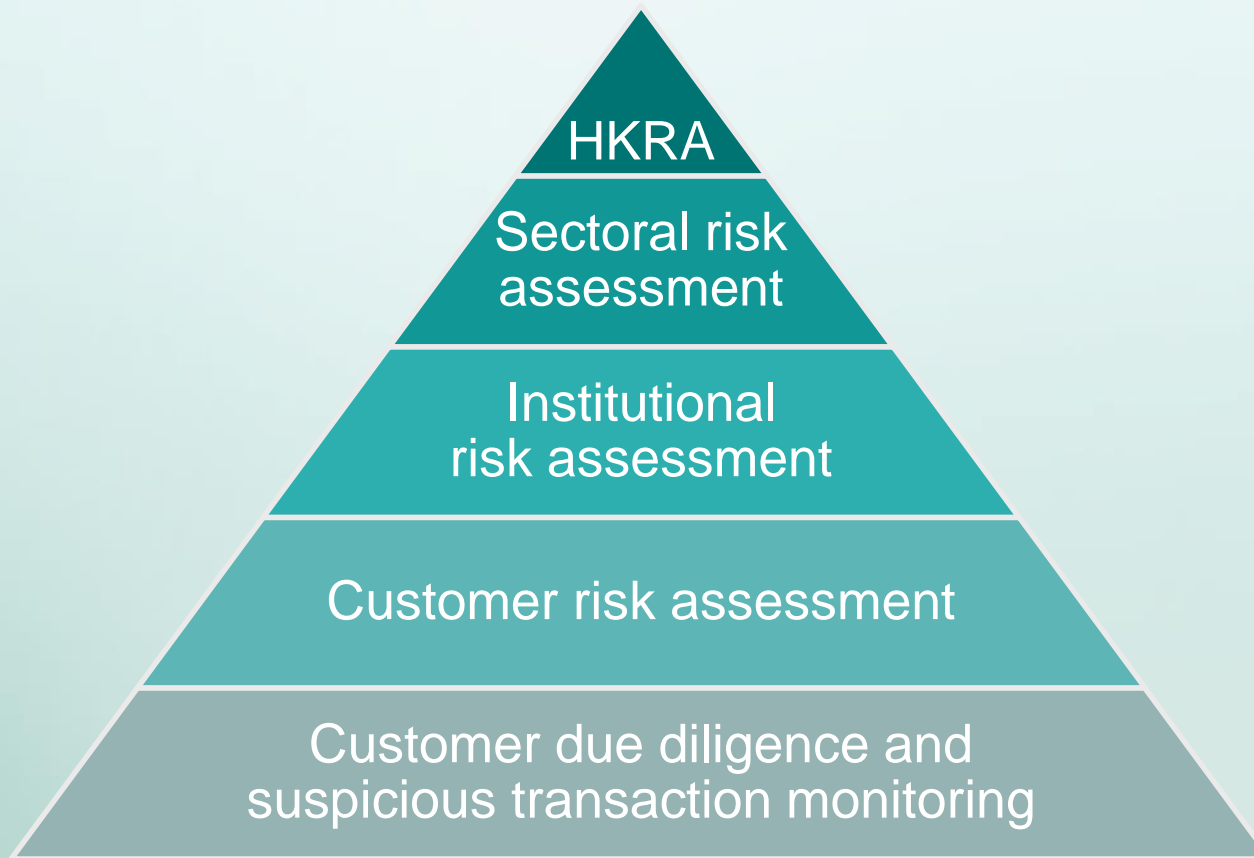
FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment

- The ML/TF risk assessment at country level are to be considered in the AML/CFT risk assessments carried out by financial institutions and DNFBPs.

👉 Institutional Risk Assessment



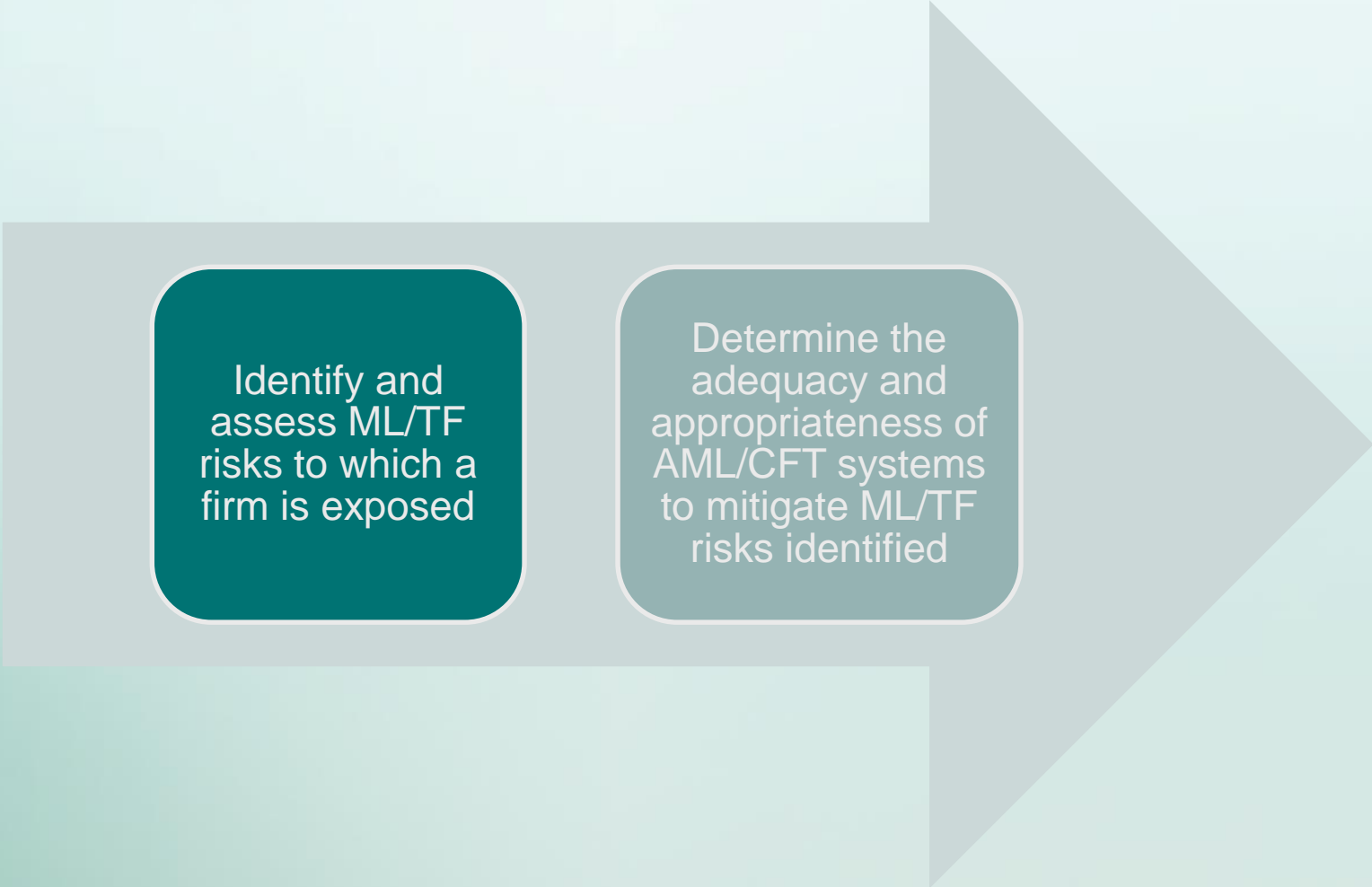
Use of the risk assessment results



A. Institutional risk assessment



Institutional risk assessment



Identify and
assess ML/TF
risks to which a
firm is exposed

Determine the
adequacy and
appropriateness of
AML/CFT systems
to mitigate ML/TF
risks identified

Institutional risk assessment (cont'd)

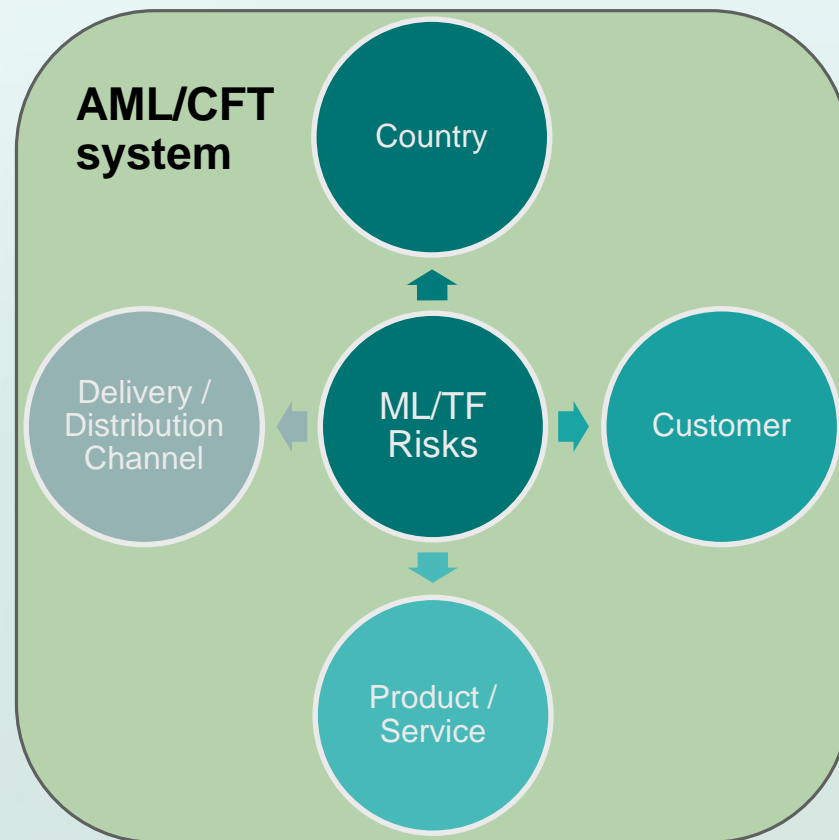
Examples of ML/TF risk factors

Customer

- Industry / Occupation
- Complexity of ownership structure (e.g. complex corporate and trust-related structures, shell companies, etc.)
- Net-worth (e.g. high net worth individuals to set up complex products and diversified portfolios in relation to tax evasion and corruption, etc.)
- PEP status

Country

- Association (e.g. country of incorporation, nationality, domicile, origination / destination of cross-border transfers, etc.) with jurisdictions that are subject to high level of organized crime, increased vulnerabilities to corruption and inadequate systems to prevent and detect ML/TF



Institutional risk assessment (cont'd)

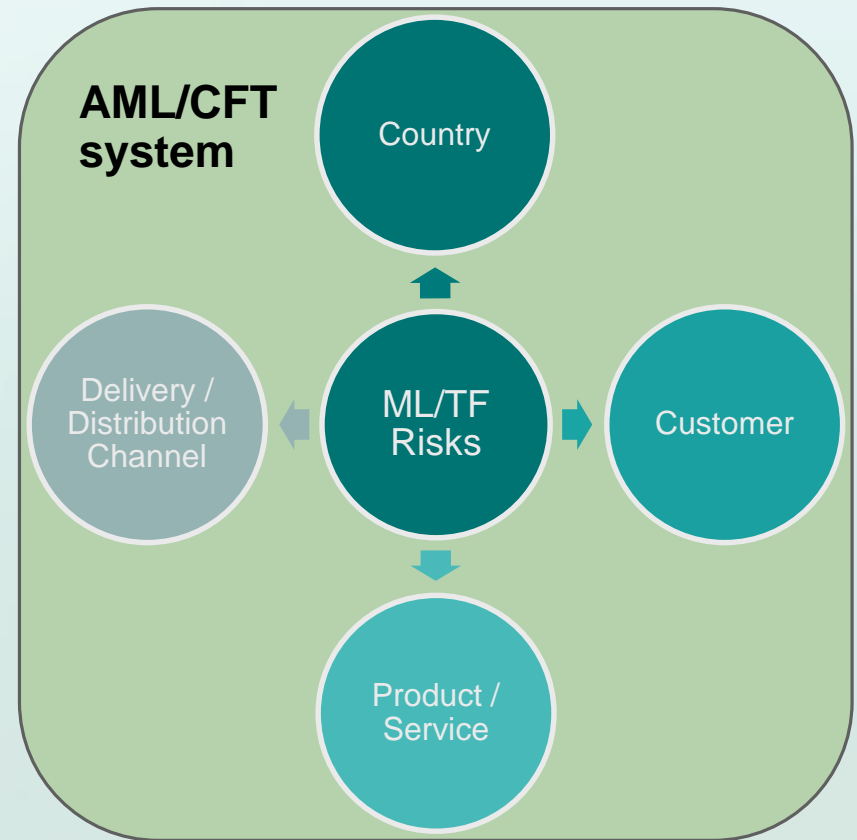
Examples of ML/TF risk factors

Product / Service

- Third party payments
- Cross border transactions
- Cash deposits
- Complex products

Delivery / Distribution Channel

- Non-face-to-face account opening



B. Customer risk assessment



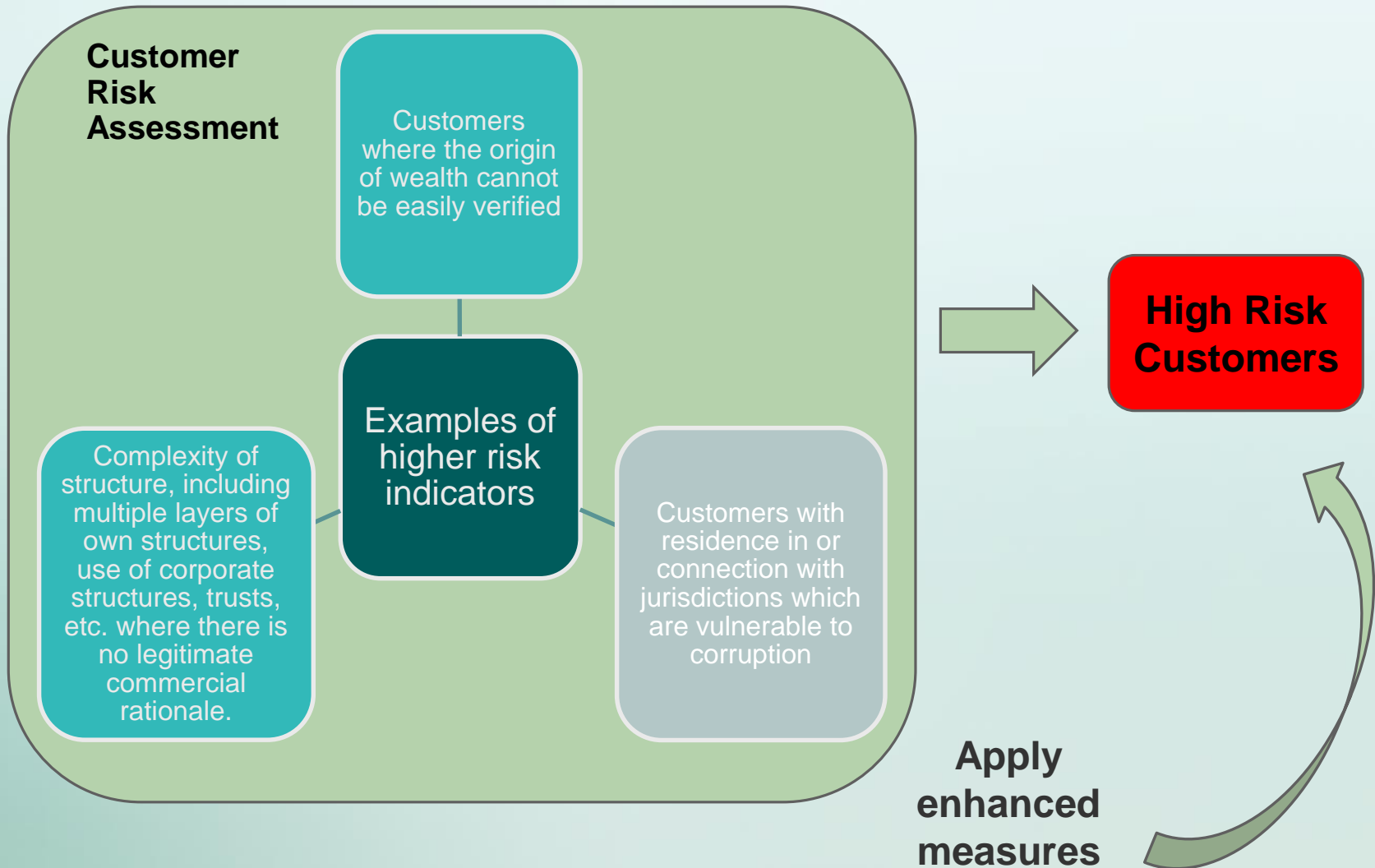
Customer risk assessment

Threats and vulnerabilities identified in the HKRA Report to be taken into account in formulating a robust customer risk assessment framework may include:

- Exposure to **non-Hong Kong customers** who may be connected with **corruption, tax evasion and other predicate offences**
- **High net-worth individuals** to set up **complex products and diversified portfolios** for ML in relation to tax evasion and corruption
- **Shell companies** are a common conduit for ML
- **Complex corporate and trust-related structures** are frequently used to conceal ownership and control of proceeds of foreign tax evasion

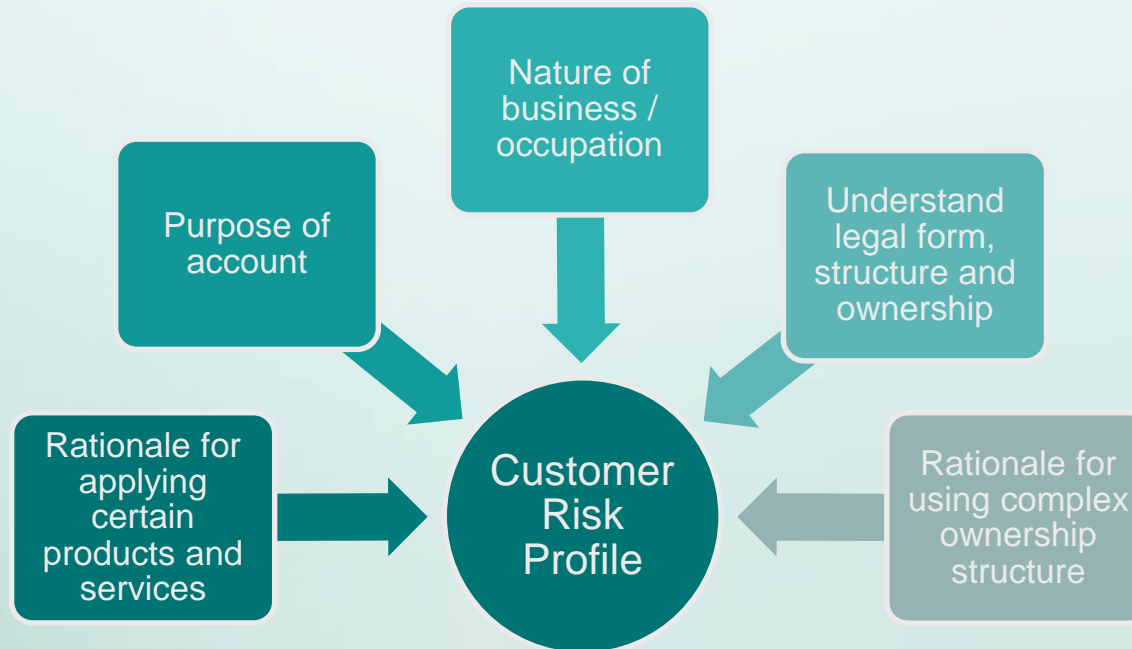


Customer risk assessment (cont'd)



Customer risk assessment (cont'd)

Obtain information to allow them to establish a customer's risk profile, for instance:



The amount and type of information and the extent to which the information is verified should be increased where the risk associated with the business relationship is higher.

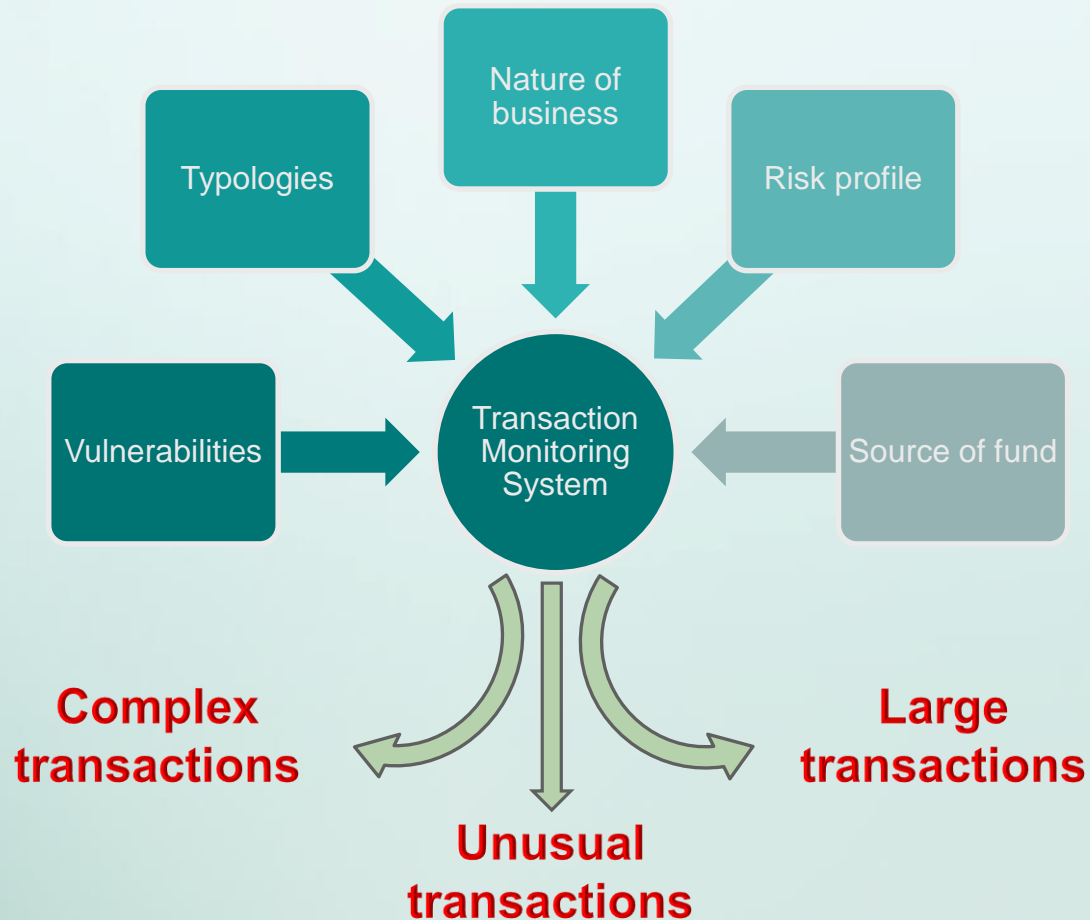
C. Suspicious transaction monitoring



Suspicious transaction monitoring

- **Typologies analysis of ML cases in the HKRA Report to be taken into account in formulating appropriate red flag indicators may include:**
 - being misused to conduct transactions constituting market misconduct (e.g. market manipulation, insider dealing, etc.)
 - cross-border transactions involving high risk jurisdictions
 - payment to or from third parties
 - use of third parties to launder proceeds generated domestically or outside Hong Kong is prevalent
 - third party ML commonly involves non-residents, students and low-paid stooges

Suspicious transaction monitoring (cont'd)



LCs should have regard to relevant examples of suspicious indicators provided in paragraph 7.14, 7.39 and 7.40 of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing.

Guidance on third party fund transfers

- Accept only upon the **receipt of approvals** from the designated senior staff member
- Take reasonable steps to **identify funds from third party sources**
- Pay special attention to **monitoring** any **frequent and/or large third party funds transfers** or **cheque payments** involved in the transactions of their customers
- **Enhanced customer due diligence** and **ongoing monitoring** should be undertaken and **additional risk-sensitive measures** be adopted to mitigate the ML/TF risks involved in cases where, for instance:
 - the customer requests payment to a third party or money is paid by a third party having no apparent connection with the customer, or
 - you are being asked to accept funds in unconventional ways, especially where non-resident customers or cross-border funds transfers are involved in those transactions or instructions.
- Conduct **appropriate enquiries** and **evaluate** what the firms know about the customer and the third party, and whether the third party funds transfers are **consistent** with the customers' known legitimate business or personal activities
- **File an STR** to the JFIU when there are grounds for suspicion
- **Provide sufficient guidance** to staff to enable them to recognize suspicious transactions irrespective of whether third party funds transfers are involved, and to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances

Source: SFC circular on Suspicious Transactions Monitoring and Reporting issued on 3 December 2013



D. Other Measures



Emerging risks

- Increasing number of reports from securities brokerages about customers' Internet trading accounts being compromised and unauthorized securities trading transactions conducted through these accounts
- Exploring the use of new technology for non-face-to-face account opening



Cybersecurity

LCs engaged in Internet trading are reminded to make reference to:

- Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading
- Circular issued on 27 October 2017 on Good Industry Practices for IT Risk Management and Cybersecurity



Non-face-to-face account opening

Achieve effective client identity verification during non-face-to-face client account opening process:

- Use of certification services provided by overseas certification authorities that meet the following criteria:
 - recognized by the Electronic Transactions Ordinance (“ETO”) (Cap.553)
 - electronic signature certificates have obtained mutual recognition status accepted by the HKSAR Government
 - the electronic signatures generated by recognized signing certificates shall have the same legal status as that of handwritten signatures within the applicable scope of the ETO in Hong Kong
- Client identity verification through professional persons or affiliates which are:
 - regulated financial institutions, certified professional accountants or notary public
- Through provision of a signed physical copy of the client agreements, a copy of client’s identity documents and identify the identity against a cheque drawn from the client’s Hong Kong bank account

Source: SFC circular on Client Identity Verification in Account Opening Process issued on 24 October 2016



Thank you

AML/CFT section of the SFC's website:

<http://www.sfc.hk/web/EN/rule-book/anti-money-laundering-and-counter-terrorist-financing/>

