



# Anti-Money Laundering and Counter-Terrorist Financing Seminar 2024

29 October 2024

## Reminders



Please carry the entry pass with you for admission and re-admission to the lecture theatre.



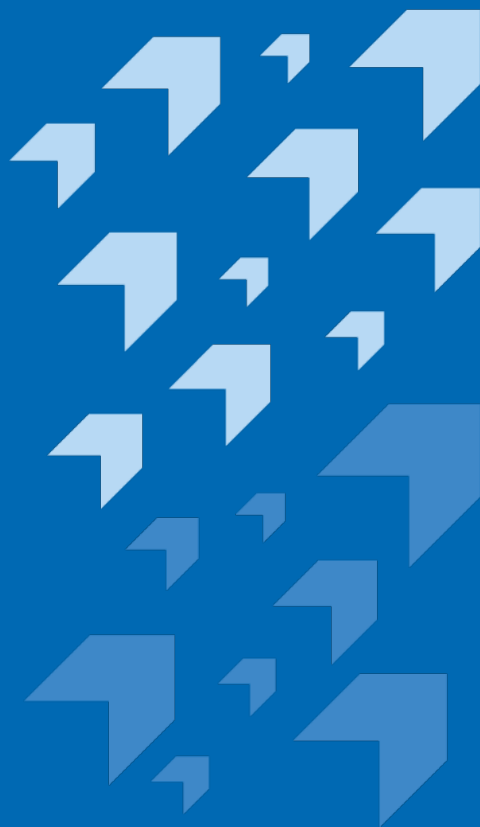
Eating and drinking is not allowed inside the lecture theatre.



Please ensure that all sound-emitting devices, including your mobile phone, are adjusted to silent mode.



Photography and video recording are not allowed.

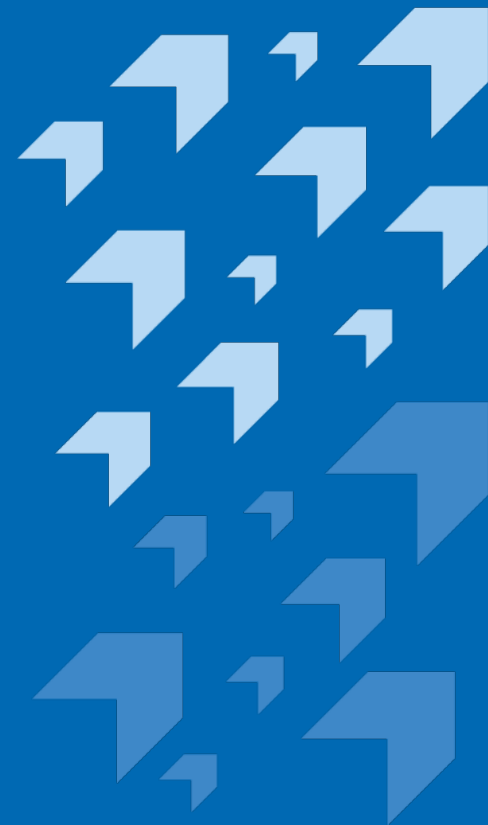




## DISCLAIMER

Where this presentation aims to enhance the audience's understanding of the topic and refers to certain requirements of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("AMLO") and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3") published by the Insurance Authority ("IA"), it provides information of a general nature and is not intended to cover all the statutory requirements that are applicable to you and your company. In any circumstances, the information and materials from the seminar should not be regarded as a substitute of any law, regulations and guidelines. Your company should seek its own professional legal advice in ensuring its compliance with the AMLO, GL3 and fulfillment of relevant regulatory obligations.

The IA reserves the copyright and any other rights in the materials of this presentation and it may be used for personal viewing purposes or for use within your company. The materials may not be reproduced for or distributed to third parties, or used for commercial purposes without prior written consent from the IA.



# Topic 1

## AML/CFT On-site Inspection Observations

**Mr Dickson Chui**  
Senior Manager  
Conduct Supervision Division  
Insurance Authority



# AML/CFT On-site Inspections

The Insurance Authority (“IA”) carried out **inspections** under section 9 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (“AMLO”) on **more than 70 insurance institutions (“IIs”)** during the period **from June 2018 to October 2024**.

## Objective



To ascertain the respective IIs’ **compliance with obligations** under **Schedule 2 of AMLO**.

## AML Guideline



The obligations are **supplemented by the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“AML Guideline”)** issued by the IA.

## Eight major areas



**01** ★  
**Senior management oversight**



**02** ★  
**Compliance functions**



**03** ★  
**Customer risk assessment**



**04**  
**Customer due diligence**



**05** ★  
**Screening of PEPs, terrorists and sanction designations**



**06** ★  
**Premium collection**



**07**  
**Ongoing monitoring**



**08**  
**Suspicious transaction reporting**

## Regulated IIs

### Carrying on long term business

- Authorized insurers
- Authorized reinsurers

### Carrying on regulated activities in respect of long term business

- Licensed individual insurance agents
- Licensed insurance agencies
- Licensed insurance broker companies

No. of IIs

**70+**

More than 70 IIs have been subjected to IA’s inspections

# Senior Management Oversight

## Understanding and mitigation of risks by senior management



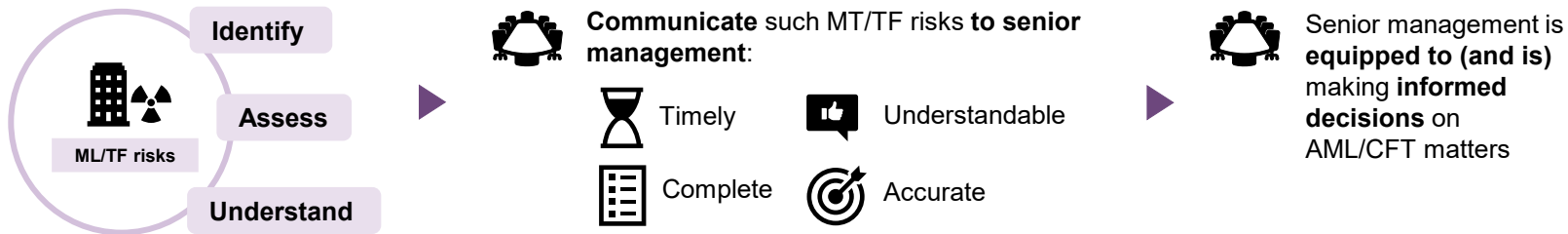
**Clear understanding** of the **ML/TF risks** to which the II is exposed



Ensure such risks are **adequately managed**

## Institutional ML/TF risk assessment (“IRA”)

An II should conduct IRA **regularly** to **identify, assess** and **understand** the **ML/TF risks** to which it is exposed.



## Significant changes to the deployed AML/CFT Systems

For any **significant changes** to the deployed AML/CFT Systems:



**Potential impact** on risks



Whether any **incremental ML/TF risks** can be **effectively addressed**





Senior management should **make informed decisions**

## Understanding and mitigation of risks by senior management






### Senior Management approval of IRA

**Approval** denotes the **taking of a decision to approve by senior management** and is an **important process** in the **taking accountability** by senior management for the **IRA and its results**.

#### Senior management



-  Have considered the IRA results
-  Subjected the IRA results to sufficient scrutiny

#### Approval process

-  Substantive
-  Evidenced
- 
-  Minutes of meeting
-  E-mail exchange

### IRA approval – Delays / Unapproved



-  **Significant delays** in submission of the IRA to senior management for approval
-  Approval from senior management was **not obtained**, even where the IRA was **presented at senior management meetings**



**Complete absence** of submission of the IRA to senior management for approval



**Ambiguity** existed **regarding which member of senior management was responsible** for **approving** the IRA results, resulted in the IRA results **going unapproved** for **several years**

# Senior Management Oversight

## Understanding and mitigation of risks by senior management

### Significant change of internal controls

Senior management should **give attention and consideration** when an II **seeks** to make a **significant change** to its **internal controls** that would **materially affect** the II's **risk exposure** to ML/TF.



**Significant increases** in the **thresholds** over which **income/asset proofs** are required for **significant sized payments**



**Significant increases** in the **thresholds** over which **payment proofs** are required to **prove** that **payments** are **not** coming from **unrelated third parties**



**Evidence** of discussion / justification



**Impact** on ML/TF risk has been **considered**



**Mitigating** supplementary controls and processes (if necessary)



**Approval** is given

### Without documenting the discussion / justification



Proceeded to implement a **materially higher threshold** for the controls but :



**Without documenting** the discussion / justification



**Without obtaining approval** from senior management



Senior management **fell short** in the **discharge** of their **obligations**

# Senior Management Oversight

## Implementation of effective AML/CFT Systems



**Identified the ML/TF risks** (through the **IRA process**)



**Senior management:**  
**Implementing effective AML/CFT Systems** (Note)



To **adequately manage** and **mitigate** those risks





# Senior Management Oversight

## Implementation of effective AML/CFT Systems

### Identifying deficiencies through compliance review

IIIs have established **internal compliance review requirements** in their internal AML/CFT policies.



**Sample testing** is commonly used in compliance review.



Compliance reviews are **adequately conducted**



**Identified deficiencies** in AML/CFT Systems



**Follow-up on action plans** to rectify the identified issues

### Weakness in oversight of compliance reviews conducted



**Senior management did not** pick up on the **lack of rigor** in the manner in which compliance reviews were being conducted on AML/CFT Systems.



**Fell short** of own internal policy



**Non-compliant practices** going undetected by such reviews



**Have not conducted** any compliance reviews in practice



Deficiencies were **not** being rectified in a **timely** manner



Eventually the **issues identified appeared** to **fall off the radar screen** altogether

# Senior Management Oversight

## Implementation of effective AML/CFT Systems

### Adequate resources



CO, MLRO and the functions supporting them



Be equipped with **sufficient resources** (as far as possible) by **senior management**



Establish **robust oversight mechanism** to ensure **effective AML/CFT Systems** are in place

### Lack of resources



Resulted in **lapses** in carrying out essential responsibilities:



Shortage of manpower



Backlogs of name screening alerts clearance



Did not carry out compliance review



Insufficient system capabilities



Failed to **follow up** the control deficiencies identified **timely**

## Data collection by the IA from 2025 onwards



Lack of resources issue



Starting to **collect relevant information** from insurers (e.g. new AML Returns to be submitted under the “Insurance Regulatory Information Connect” platform)

# Compliance functions



IIs



Develop own  
AML/CFT controls  
and procedures



Address specific  
ML/TF risks (as  
identified in IRA)



To achieve **compliance** with  
the requirements in **AMLO** and  
the **AML Guideline**

## Responsibilities of the Compliance Officer (“CO”)



**Developing** and **continuously reviewing** AML/CFT Systems to ensure such systems to:



Remain **up-to-date**



Meet **current statutory and regulatory requirements**



Be **effective** to manage  
ML/TF risks of the II



**Overseeing** all aspects of the II's AML/CFT Systems, which include **monitoring effectiveness** and enhancing controls and procedures.



**Communicating** key AML/CFT issues with **senior management**, including any **significant compliance deficiencies** identified.



# Compliance functions

## Developing and continuously reviewing the AML/CFT Systems

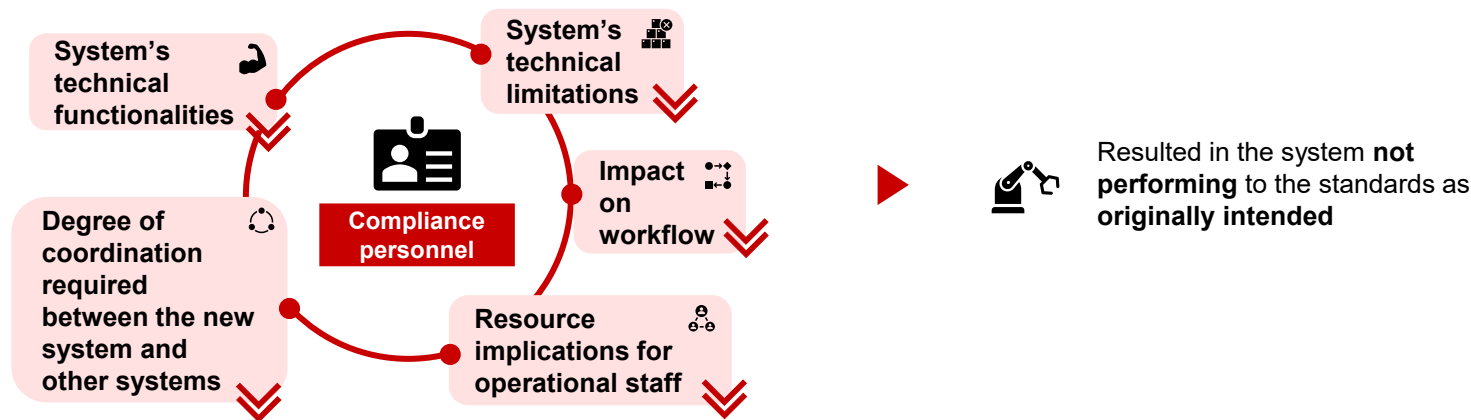
When deploying **new technology-based AML/CFT systems**, the compliance function should:

- ✔ Should be **sufficiently resourced**
- ✔ Should **cooperate with** and have **full support** from other relevant functions (e.g. Information Technology (“IT”) department and Operations departments)

## System not performing to the standards as originally intended



Deployed a **new technology-based AML/CFT system**



# Compliance functions

## Monitoring effectiveness of AML/CFT Systems

### Sample testing



A **commonly used** control measure to evaluate AML/CFT controls and processes



Ensure **early detection** of control weakness

### Weakness identified through sample testing

Compliance function:



Draw to the attention of the **relevant operating unit** in the II



Draw to the attention of **senior management**, where appropriate



**Follow up until remediated**

# Compliance functions

## Monitoring effectiveness of AML/CFT Systems

### Weakness / Absence of sample testing

Compliance functions were **not conducting sample testing** to ensure **early detection of control weakness**:



On a **sufficiently regular** basis



On an **extensive** basis



**Deficiencies** in the functioning of certain **AML/CFT controls and processes** in particular operations of the IIs:



Going **undetected**, sometimes for **prolonged periods**

### Heavy reliance of incident reporting protocol



Inadequacies going **unidentified**



Inadequacies **not reported to senior management**

# Compliance functions

## Communicating key AML/CFT issues with senior management



### A call for complete transparency

To **report** identified AML/CFT deficiencies **upwards** to **senior management**.



#### Purpose

- ✓ To keep senior management **apprised** of emerging issues
- ✓ **Early actions** can be taken

#### Reporting upwards

-  Report upwards in a **timely manner**
-  Presented **factually** and **without spin**

### The Compliance Officer (“CO”)

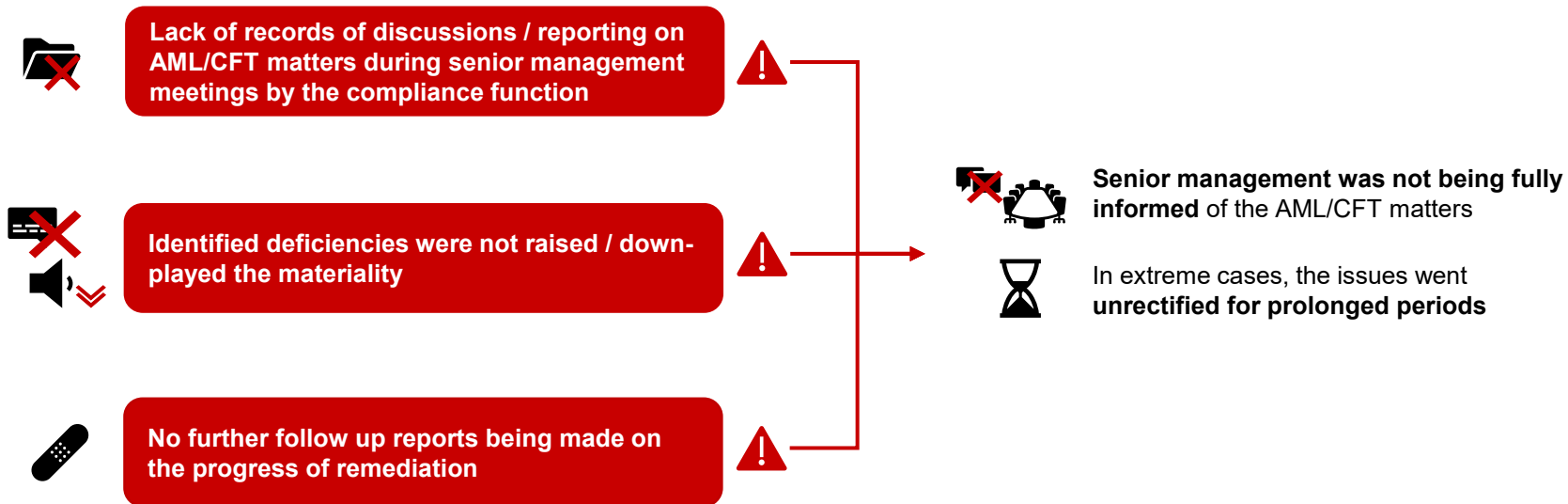
-  Strong integrity
-  Courage



Raise issues which need **rectifying** to senior management in a **timely** and **factually accurate manner**

# Compliance functions

## Communicating key AML/CFT issues with senior management






# Customer risk assessment

## Customer risk assessment (“CRA”)

 To **assess** the **ML/TF risk level** associated with a **proposed business relationship**

 Conducted at **initial stage** of the CDD process, **determines** the **extent** of **CDD measures** to be applied



### Lack of risk assessments in practice

- **Unable** to produce any **documentary evidence**
- **Not** doing it **consistently** for all customers



### Risk assessment results unavailable at the time of new business

- Due to **system limitation**
- **High risk customers** were **not** being **subjected to enhanced due diligence measures**

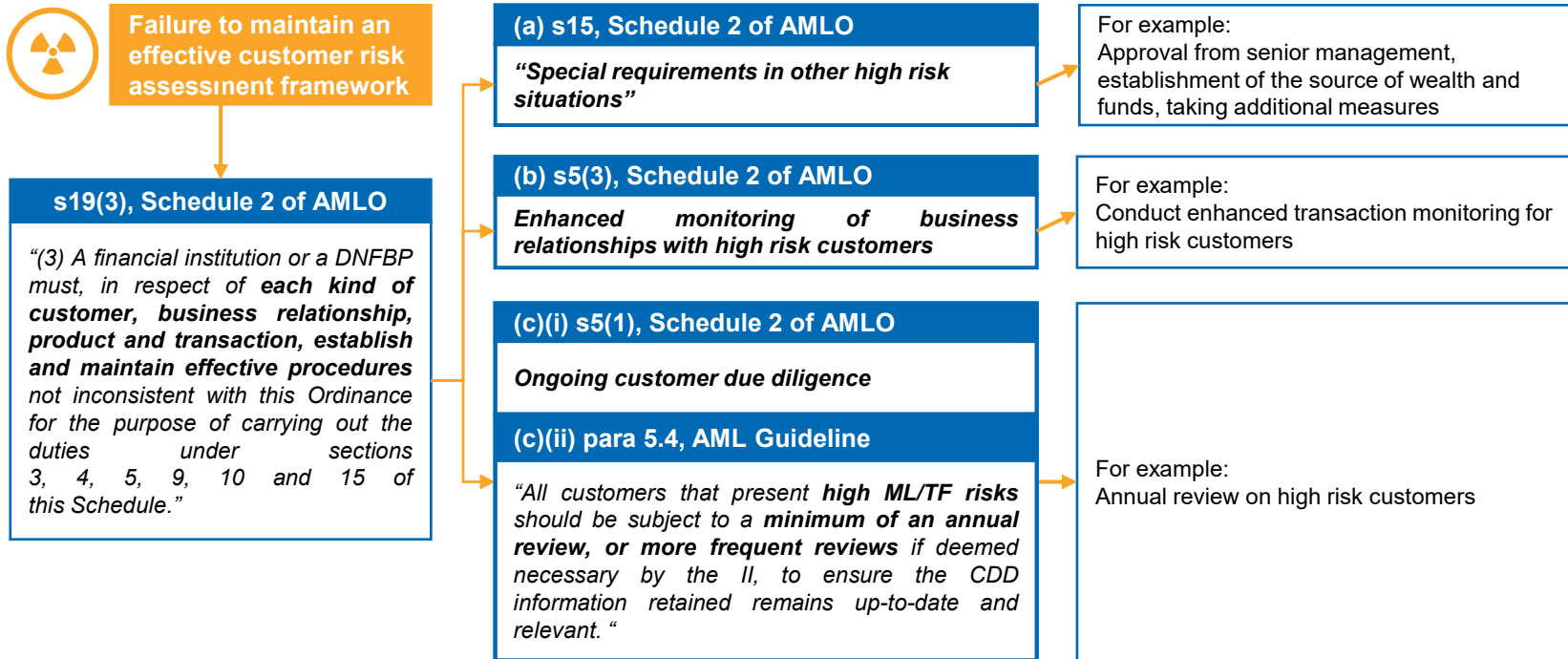


### No risk assessments for change of policy ownership

- For **new policyholders** of existing policies



# Cascading effect arising from failure to maintain an effective customer risk assessment framework



# Screening of PEPs, terrorists and sanction designations



To establish and maintain **effective procedures** for determining whether a customer or a beneficial owner is a **PEP**



A requirement to **screen** for **terrorists** and **sanction designations**



**Ineffective screening systems** may **hinder the ability** to identify (potential) customers who may be **PEPs, terrorists** and **sanction designations**



## Ineffective algorithm design and calibration of system settings

- **Misappreciation** of algorithm, systems and databases
- Resulted in screening systems being **insufficiently sensitive**



## Wrongful clearance of alerts

- Concluded / Closed actual PEP alerts as being **false positives**
- **Without any** documented review notes



## No screening on beneficial owners

- On an **ongoing basis**
- Information of **beneficial owners** was **not captured** in the system



# Use of Suptech by the IA for assessing name screening effectiveness (screening system tool)



## Use of Suptech by the IA



To **test** and **validate** the II's **name screening system(s)** more effectively.



Focus on the **reasonableness** of parameters and **thresholds** adopted.



## The IA independent testing



**Publicly available data** on sanction designations / PEPs is used.



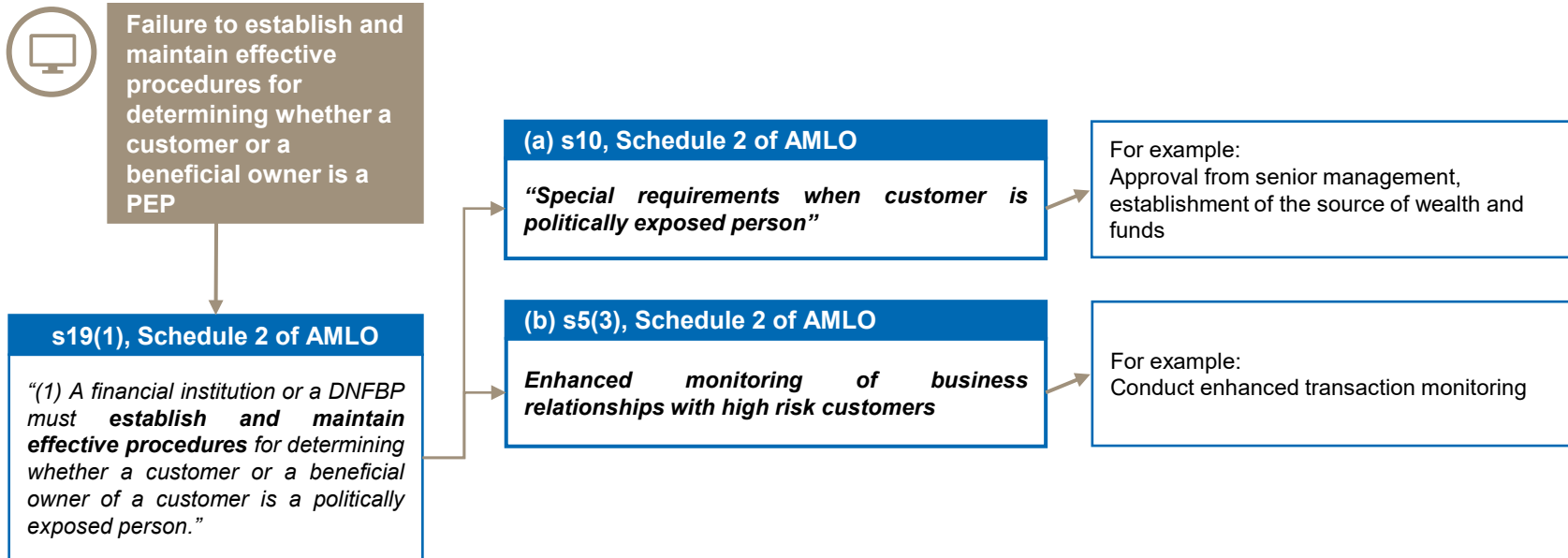
The testing of the system(s) would be carried out in a **testing environment** which **exactly replicates its production environment** and **production settings**.



**Full set of screening results** inclusive of all alerts generated by the II's screening system(s) would be returned to the IA for analysis.



# Cascading effect arising from failure in screening of PEPs, terrorists and sanction designations



# Premium Collection

## Unrelated third-party payments

### Premium payments made by cashier order

Threshold approach:



To obtain **payment proof**



For the purpose of **ascertaining** the **payment** was coming **from the policyholder** (but not from an unrelated third-party)



Above  
threshold



Demand **comprehensive proof** of the **person** who **purchased** the **cashier order** to make the payment



Below  
threshold



**Self-declaration** by the policyholder



**Sample testing**

### False declaration



The cashier order was **not purchased** by the **policyholder**, but from:



**Other person's** account



**Insurance agent** (who even **witnessed** the policyholder signing the self-declaration, **knowing** it to be **untrue**)

### Circular issued by the IA

For details of the IA's expectation on **enhanced controls on premium payments by cashier orders**, please refer to the **circular** issued on **9 April 2024**.

[https://www.ia.org.hk/en/legislative\\_framework/circulars/antimoney\\_laundering/files/Cirdd9.4.2024.pdf](https://www.ia.org.hk/en/legislative_framework/circulars/antimoney_laundering/files/Cirdd9.4.2024.pdf)

## Communication Tools

**IA** Depending on the **level of deviation** which the regulatory requirements observed, the three main **communications tools** are utilized by the IA:



To **record** the IA's **observations**



To **present** the **observations** to IIs



To use as a basis for **follow up** so that **rectification** is **achieved**

**1**

**Management letter**

The divergences from the regulatory requirements are slight and **not of an elevated level of seriousness** but in any event need to be addressed in order for the II to stay on the right compliance track.

**2**

**Compliance Advice Letter (CAL)**

To highlight deviations observed from the regulatory requirements which are likely non-compliances, albeit they are deemed to be **of a lesser serious nature** at the time the observation is made.

To admonish the II to correct its course (and rectify) in a short but realistic time frame, so as to prevent the issues cited manifesting to become serious non-compliances.

**3**

**Letter of Concern (LC)**

Warning!

To highlight the non-compliant practices observed which are **of a more immediate concern** and that need to be rectified or eliminated in the very near term.

Not only cautions the recipient to cease and immediately eliminate the identified practices, but also warns that failure to heed the caution (or any repeat of the non-compliances going forward) will be taken into account in determining the severity of any disciplinary penalty to be imposed in the future.

## Communication Tools

IIs



To **outline the remedial actions** it will be taking (or which it has taken)



For **rectification of deficiencies**



Within a **reasonable timeframe**

Depending on the circumstances, the II may also be invited to conduct **independent review** by:



**Internal** audit function



**External** party



**Validate the completion and effectiveness** of the **remediation taken**







**Follow up** with the II **until** the II **confirms remediation** has been **completed** and **evidences** the remediation.



# Post-inspection matters

## Disciplinary Actions

### Non-compliances with the regulatory requirements that are so obviously evidenced

-  Non-compliances are **obvious**, of a **prolonged** or **systemic nature**
-  Show **Inherent weaknesses** in **governance**
-  Go **beyond just technical** given their **scale**
-  **Cannot be considered inadvertent** because they were **known within the II** and **rectification** has either been **continually delayed** or **not been undertaken**






The matter has to be dealt with by the **disciplinary process**



The **non-compliance(s)** needs to be **penalized**

### In situations where the disciplinary context needs to be initiated

The IA will **follow up** with the II to ensure the II **rectifies the matters as quickly as possible**.

-  **Level of cooperative attitude** the II demonstrates
-  **Early acceptance** of and **contrition** the II shows for the matters identified
-  **The way the II displays** how seriously it takes such matters



Can be **take into account** to **mitigate any level of eventual disciplinary action**

# Further information

## AML seminars / webinars since 2011

Date	Details	Presentation Materials
21 November 2023	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Major updates on the Guideline on Anti-Money Laundering and Counter-Terrorist Financing and other compliance matters</a></li> <li><a href="#">Proliferation Financing Risk Assessment and Mitigation</a></li> <li><a href="#">Suspicious Transaction Report</a></li> </ol>
8 December 2022	Anti-Money Laundering and Counter-Terrorist Financing Webinar	<ol style="list-style-type: none"> <li><a href="#">Proliferation Financing Risk Assessment and Mitigation</a></li> <li><a href="#">Suspicious Transaction Report</a></li> <li><a href="#">Money Laundering and Terrorist Financing Methods and Suspicious Transaction Reporting</a></li> <li><a href="#">Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report 2022 and other AML/CFT Compliance Matters</a></li> </ol>
7 December 2020	Online Sharing Session: Key Observations of Insurers' AML/CFT Control on Virtual Customer Onboarding	<a href="#">Key Observations of Insurers' AML/CFT Control on Virtual Customer Onboarding</a>
21 October 2019	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Mutual Evaluation Report of Hong Kong</a></li> <li><a href="#">Suspicious Transaction Reporting</a></li> <li><a href="#">Recent Update of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing</a></li> </ol>
5 June 2018	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report (Part 1)</a></li> <li><a href="#">Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report (Part 2)</a></li> <li><a href="#">Regulatory Update and Supervisory Observations on AML/CFT</a></li> <li><a href="#">Suspicious Transaction Reporting</a></li> </ol>

31 May 2018	Briefing Session: Key Findings of AML/CFT Onsite Inspection Visits to Authorized Insurers Carrying on Long Term Business	<a href="#">Key Findings of AML/CFT Onsite Inspection Visits to Authorized Insurers Carrying on Long Term Business</a>
22 November 2017	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Regulatory Update and Supervisory Observations on AML/CFT</a></li> <li><a href="#">Suspicious Transaction Reporting</a></li> </ol>
1 December 2016	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">AML/CFT Transaction Monitoring – Principle and Practice</a></li> <li><a href="#">Suspicious Transaction Reporting</a></li> </ol>
9 November 2015	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Hong Kong's Regulatory Regime on AML/CFT</a></li> <li><a href="#">Compliance issues on AML/CFT</a></li> <li><a href="#">Suspicious Transactions Reporting</a></li> </ol>
9 October 2014	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Characteristics of an effective AML/CFT System</a></li> <li><a href="#">Suspicious Transaction Reporting</a></li> </ol>
17 October 2013	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Implementation of an effective AML/CFT system</a></li> <li><a href="#">STR Reporting</a></li> </ol>
14 September 2012	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Key Aspects of an AML/CTF system</a></li> <li><a href="#">Anti-Money Laundering by STR Reporting</a></li> </ol>
1 March 2012	Briefing Session: Guideline on Anti-Money Laundering and Counter-Terrorist Financing	<a href="#">Guideline on Anti-Money Laundering and Counter-Terrorist Financing [Text Version]</a>
15 December 2011	Anti-Money Laundering and Counter-Terrorist Financing Seminars	<ol style="list-style-type: none"> <li><a href="#">Building a Robust Regime on Anti-Money Laundering and Counter-Terrorist Financing [Text Version]</a></li> <li><a href="#">Suspicious Transaction Report</a></li> </ol>

<https://www.ia.org.hk/en/supervision/antimoneylaundering/referencematerialsandrelevantwebsites.html>

## Frequently Asked Questions ("FAQs") in relation to AML/CFT

### Anti-Money Laundering and Counter-Terrorist Financing


**Important Note:**

Frequently Asked Questions ("FAQs") in relation to Anti-Money Laundering and Counter-Terrorist Financing ("AML/CFT") below do not form part of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the Insurance Authority ("Guideline"). The FAQs are designed to be read in conjunction with the Guideline, and the key terms and abbreviations used have the same meanings as in the Guideline.


Q1 to Q2:	AML/CFT Systems
Q3 to Q5:	Identification and verification of identity – natural persons
Q6 to Q10:	Identification and verification of identity – legal persons
Q11 to Q13:	Identification and verification of identity – trusts or other similar legal arrangements
Q14 to Q16:	Recognized digital identification system
Q17 to Q20:	Reliability of documents, data or information
Q21:	Connected parties
Q22 to Q24:	Beneficial owners
Q25 to Q27:	Ownership and control structure
Q28 to Q30:	Person purporting to act on behalf of the customer (PPTA)
Q31 to Q32:	Simplified due diligence
Q33 to Q34:	Enhanced due diligence
Q35 to Q36:	Politically exposed persons
Q37 to Q38:	Customer not physically present for identification purposes
Q39:	Intermediaries
Q40 to Q41:	Transaction monitoring
Q42:	Record-keeping



# Thank You

 (852) 3899 9983

 [www.ia.org.hk](http://www.ia.org.hk)

 (852) 3899 9993

 蓋世保鑑 Insurpedia

 [enquiry@ia.org.hk](mailto:enquiry@ia.org.hk)

