保險業監管局
Insurance Authority

Anti-Money Laundering and Counter-Terrorist Financing Seminar 2025

27 October 2025

保險業監管局
Insurance Authority

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.

Topic 1

Common Issues and Good Practices of Three Lines of Defense in Implementing AML/CFT Controls

Mr Dickson Chui
Senior Manager
Conduct Supervision Division
Insurance Authority

Mr Joseph Lee
Deputy Senior Manager
Conduct Supervision Division
Insurance Authority

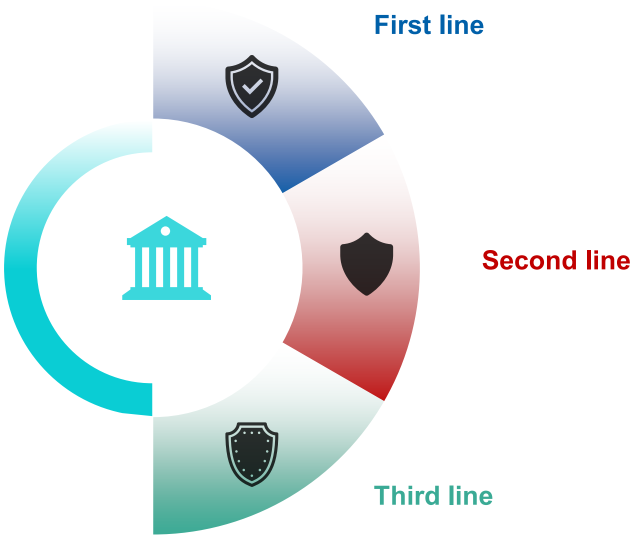
Three lines of defense

The three lines of defense and their roles and responsibilities in AML/CFT compliance

Three lines of defense

Each function has their:

- Different roles and responsibilities
- Unique challenges



Three lines of defense

The three lines of defense and their roles and responsibilities in AML/CFT compliance

First line

Own and **manage** risks associated with day-to-day operational activities.

Departments (examples):
- Underwriting
- Policy Admin
- Claims
- Cashier
- Information technology (IT)
- Finance
- Frontline personnel, technical representatives

Second line

Identify and **manage emerging risks** in daily business operations.

Provide **compliance** advice and oversight.

Department (example):
- Compliance (including Compliance Officer and Money Laundering Responsible Officer)

Third line

Provide **independent** and **objective** assurance.

Assess whether the first line and second line functions are **operating effectively**.

Evaluate compliance programs by carrying out **testing** and **validations**.

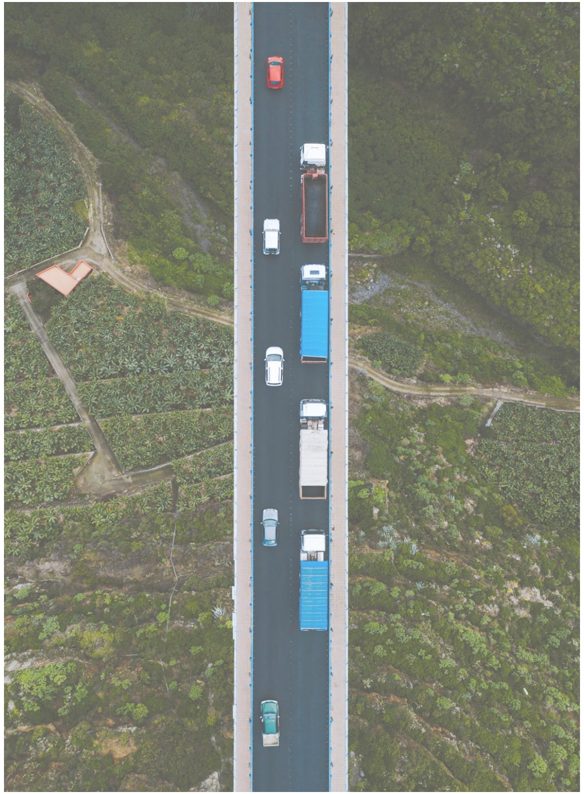
Department:
- Internal audit

Tone at the middle

Middle managers

Have the **most frequent** and **direct contact** with frontline staff

Observe the actual practice with **greater clarity**



First line – Common Issues

保險業監管局
Insurance Authority

Inconsistency of practices between different departments

Misalignment of practices (examples):

Customer Risk Assessment ("CRA")

Customer Due Diligence ("CDD")

Underwriting

- CRA methodology 1
- CDD requirements 1

Policy Admin

- CRA methodology 2
- CDD requirements 2

Possible causes:
Ineffective communication between siloed teams

Shortcomings in carrying out AML/CFT duties

Policies and procedures **are not adhered** in practice

Lack of vigilance in reporting suspicious transactions

Dismissal of alerts **without documentation**

Approval of high risk cases by **junior staff**

Possible causes:

Conflicting priorities

Fast-paced work environment

First line – Common Issues

Ineffective oversight and quality control of outsourced functions

Insufficient oversight

Critical process has been **overlooked**

Possible causes:

A mindset that they **do not need to bear responsibility of the failures** of the outsourced functions

First line – Observed Good Practice

1.5 line of defense

- A **bridge** between first line and second line
- Provide **risk training**, **control assurance** and **advisory services** to the first line

Outsource with:

- **Ownership** of the process
- **Good** quality control
- **Frequent** feedback

Second line – Common Issues

Unclear policies and procedures

Policies and Procedures

- **Lack** essential elements
- **Unclear** direction

Possible causes:

- **Inadequate knowledge** of **AML**
- **Inadequate understanding** of the **risks** faced by the company

Inadequate compliance control testings

The compliance control testings are inadequate:

- **Not focused** on high risk areas
- **Unable to detect** critical failures
- **Not** on a **timely** basis

Possible causes:

- **Inadequate understanding** of the company's **AML/CFT control processes** and **capabilities of the systems in place**
- **Unwilling** to assess complex issues

Second line – Common Issues

Failures in critical AML/CFT processes

Development of critical AML/CFT processes:

Algorithms **Parameters**

~~**Second line**~~

Leave it to first line **without overseeing** them

Resulting in **failures**

Possible causes:

- **Unclear / limited ownership** on AML/CFT systems
- A **false belief** that they **do not bear responsibilities** if they have **not** been directly involved in the tasks
- **Ostrich effect**

Second line – Common Issues

Insufficient resources allocated to AML initiatives

Insufficient resources (examples):

Training

Technology

Systems

Possible causes:

- **Lack of support** from **senior management**
- **Compliance function** is **not prioritized**

Difficulties in implementing changes

Difficult to **enforce** compliance policies

Difficult to **implement** necessary changes

Hinder the effectiveness of AML programs

Possible causes:

- **Inadequate authority / seniority** to exert influence on first line staff
- **Lack / little support** from first line staff

Second line – Observed Good Practice

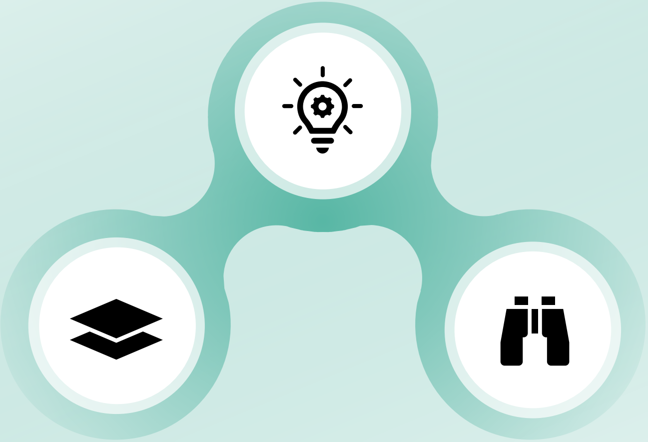
Dedicated Financial Crime Compliance ("FCC") / AML teams overseeing AML/CFT compliance

Adequate resources are allocated

Note: IA's annual AML return asks insurers to evaluate whether their identified inadequacies in AML/CFT systems were primarily attributed to a shortage of human resources.

Third line – Common Issues

Not leverage on latest technology



Lack the **technical knowledge** in AML/CFT

Not assessing AML issues **holistically** / **Not** forward-looking

Compliance review and audit testing

Paragraph 3.4 of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3") issued by the Insurance Authority ("IA"):

> An Insurance Institution ("II") should implement **AML/CFT Systems (i.e. AML/CFT policies, procedures and controls)** having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, and which should include, inter alia:
>
> - compliance management arrangements
> - an independent audit function

Compliance Department

Second line of defense.

A **pivotal party** in carrying out the review on first line AML operations.

Carry out **compliance review**

- Usually being formulated as a **key component** in **compliance management arrangement**.

Internal Audit Function

Third line of defense.

Established to perform **periodic reviews** of both first line (i.e. operations) and second line (i.e. compliance).

Carry out **audit testing**.

Compliance review and audit testing – Good Practice

Compliance Department (second line of defense) and Internal Audit Function (third line of defense)

Collaborate with each other to **support the senior management** in implementing effective AML/CFT Systems that can adequately manage the ML/TF risks identified:

- **Aligning** ML/TF risk assessments but not duplicating the efforts
- Developing **concerted** compliance and audit testing plan for AML/CFT Systems and presenting it to the appropriate committee **for approval**
- Executing **a holistic review approach** by coordinated monitoring & testing or even a having joint testing of key controls to enhance efficiency

Note: The internal audit function shall maintain its independence and the collaboration must not impair their integrity and objectivity in formulating their audit plan and scope.

Risk-based testing plan

A comprehensive risk-based testing plan

AML/CFT Systems should be **one of the essential components** in an II's audit and compliance testing plan.

Assists an II to **monitor** AML/CFT controls effectiveness, **enhance** the procedures and **address** an II's most pressing issues on high-risk areas.

Before formulating and updating the testing plan

The reviewer is expected to evaluate and review **thoroughly the II's institutional risk assessment** to identify and analyze the ML/TF risks.

The significance of relevant regulatory risks are typically assessed in terms of **impact** and **likelihood**.

Enables the reviewers to **properly align** and **focus on key areas based on limited resources.**

Risk-based testing plan – Good Practice

The IA

Periodically share general lessons learnt in its inspections through seminars, training and circulars.

The latest circular on general observations from AML/CFT inspections was issued in May 2025.

Gap Analysis

Most of the IIs would use the IA's general observations to perform a **health check** or **gap analysis** against their current AML/CFT control procedures.

Highly recommended:

Embedding them into their risk assessments for compliance and audit testing plan by prioritizing high-risk areas for monitoring.

Review on AML procedures and walkthrough interviews

保險業監管局
Insurance Authority

Reviewers should, first of all:

Understand the **regulatory AML/CFT requirements**

With reference to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (“AMLO”), the IA’s AML/CFT Guideline (i.e. GL3), circulars and FAQs.

Understand II’s **AML/CFT Systems (i.e. policies, procedures and controls)**

Reviewing its AML/CFT procedure documents.

Conducting walkthrough interviews with first line (i.e. operations) or second line (i.e. compliance) (if applicable) to understand the entire processes in practice.

Walkthrough interviews

Assist the reviewers to gain a thorough understanding on:

- The **prevailing AML/CFT requirements**
- The II’s **existing AML/CFT controls**

Review on AML procedures and walkthrough interviews – Good Practice

保險業監管局 Insurance Authority

Walkthrough interviews

Subject to the testing scope, reviewers may perform the following to the first line operations **before** interviewing them:

- Lay out **walkthrough areas**
- Communicate **in-scope areas**

Highly recommended:

- Systems demonstration sessions, accommodating reviewers better to **visualize** the whole step-by-step processes

Review on AML procedures and walkthrough interviews – Good Practice

保險業監管局
Insurance Authority

Example of walkthrough areas (non-exhaustive)

To understand the AML/CFT controls of a typical Underwriting Department of a life business insurer.

- Data capture
- Customer Risk Assessment
- Financial transactions
- Customer Due Diligence
- Screening
- STRs

Customer Risk Assessment – Sample questions:

- What are the predefined risk factors?
- How is a customer's risk level derived and calculated (e.g. factor approach, scoring approach)?

Customer Due Diligence – Sample questions:

- How does the Underwriting Department apply CDD measures to diverse new customers presenting different levels of ML/TF risk?
- What CDD documents are being obtained?
- Who are the designated personnel granting the senior management approval?

STRs – Sample questions:

- What are the current reporting protocols for staff to report suspicious transactions?

Work Programs & Good Practice

保險業監管局
Insurance Authority

Work programs

Understanding and reviewing the AML/CFT Systems

It is common for reviewers to build work programs:

- **details of tasks** and **methodologies** that would be used to achieve the testing objectives.
- **analysis and evaluation** to develop findings, conclusions and recommendations.

Good Practice

Collaborate to identify the perceived ML risks and controls (NOT testing steps) in the work programs.

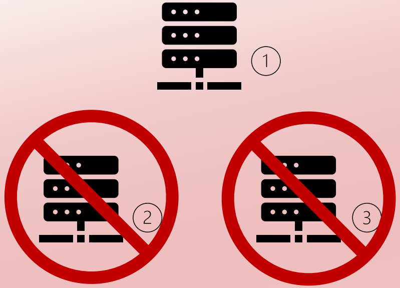
Operations (first line) — Compliance (second line)

Note: The Reviewer should maintain independence and the collaboration must not impair integrity and objectivity in formulating their work program.

Specifically:

- The **names of the reviewers / approvers** who would complete / review the work
- The **date** the work was completed

Work Programs – Common Issues



An II was generating AML exception reports from **different operating systems** for transaction monitoring purposes.

Compliance Review **only covered reports in one system** but not the others.

Certain AML exception reports have **never** been within the testing scope.

Meanwhile, the IA inspectors noted there were **severe deficiencies** on those **out-of-scope exception reports.**

An II was performing a Compliance Review on transaction monitoring and name screening.

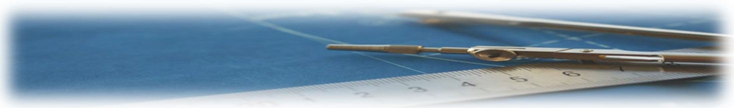
IT data generation logic and parameters used were set to be **out-of-scope without any justifiable reasons behind**.

Without the underlying data generation logic tested, the **effectiveness of these AML control areas** which were particularly highly dependent on the accuracy of system design and data extraction logic **could not be reasonably ascertained**.

Testing execution – Control design & Common Issues

Control design

Document the evaluation of the adequacy of the AML/CFT control design



May consider if implemented control, **individually or in combination** with other implemented controls:

Capable of effectively preventing or detecting and correcting deficiencies that could result in control failures?

Common issues

Staff responsible for **designing** the system logic for critical AML processes are system developers who may **not** have expertise on AML

Lack understanding of the AML controls and name screening process

Inadequate UAT was carried out **by end users** (e.g. first line operations, second line compliance)

User Acceptance Test (UAT)

A **critical** process.

Is imperative that **first line (i.e. operations)** and **second line (i.e. compliance)**:

- fully conversant
- engage in that process to throw multiple real-life scenarios at the system in a quasi-production environment to **test its limits** and flush out problems.

Testing execution – Control effectiveness

保險業監管局
Insurance Authority

Test of controls by evidence

An evaluation of the existing controls to assess whether those controls are properly in place.

Example **(for illustration only)**

To evaluate whether suspicious transactions are promptly escalated to the Money Laundering Reporting Officer and reported to JFIU accordingly

Reviewers to **conduct walkthrough interview** with first line staff:

- **assess their understanding** of when and how to identify and report suspicious transactions
- whether they have **good understanding** of the relevant in-house procedures
- select **REAL CASES** (no matter whether reporting to JFIU or not) for **testing:**
  - to evaluate the end-to-end reporting process and identify potential control gaps

Testing execution – Control effectiveness

保險業監管局
Insurance Authority

Sampling

A useful tool to **evaluate control effectiveness** of transactions with **large populations.**

To provide a **reasonable basis** to draw conclusions about **the population** from which the samples are selected.

Random sampling

Sample items are selected in a way that each sampling unit has a **known probability** of being selected.

Example:
Random number generators, for example, random number tables

Systematic sampling

The number of sampling units in the population is **divided** by the sample size to give a sampling fix interval.

Target sampling

The reviewers shall apply **judgment** to select sample items.

Testing execution – Control effectiveness

Reperformance

Involves the reviewer, acting as an **independent party** to **execute controls** to check if they are effective.

Using **data analytics** software or even as simple as spreadsheet templates.

Example (for illustration only)

A reviewer to **reperform** a **specific transaction monitoring rule** assessing whether alerts are being generated as intended.

To validate the accuracy and effectiveness of the rule logic.

Monthly monitoring report with parameters.

Independently extract the relevant policy and financial transactions in a list from an operating system.

Using **data analytics** to **re-perform** and filter out transactions (using formula) accordingly to ensure all filtered transactions are **properly captured** in the report.

Case study – Compliance review on transaction monitoring reports

保險業監管局
Insurance Authority

Objective setting

To assess the **accuracy and completeness** of monthly transaction monitoring reports of frequent policy ownership changes with material payouts.

Scope

Transactions monitoring reports in the past 6 months, from 1 January 2025 to 30 June 2025.

Includes assessment of the **report generation logic**, **data accuracy**, **completeness** of exception identification.

Collect and Review information

Collect the information via walkthrough interviews with staff in first line operations **ahead of** the testing:

- System configuration and data of insurance policies, policyholders and payment transactions in **life policy system**
- Functionality and controls of the **transaction monitoring system** used to generate monthly monitoring reports

Testing procedures

To be continued in next slides.

Case study – Compliance review on transaction monitoring reports

保險業監管局 Insurance Authority

Testing objective

To evaluate whether requisite data from source system (i.e. life policy system) is **properly extracted** and **completely transferred** to transaction monitoring system.

This may include ensuring proper controls over **data transfer reconciliation**, **exception handling** and **audit trail**.

Testing procedures

Test 1: System data extraction and transfer

Testing approach

Conduct **walkthrough interviews** with IT and Operations departments to **corroborate** on data fields and transfer among the systems.

Examine **control design** to identify any deficiencies in data field availability.

Data transfer reconciliations that may impair data completeness, exception detection and thus hindering system workflows.

Case study – Compliance review on transaction monitoring reports

保險業監管局 Insurance Authority

Testing procedures

Test 2: System logic and parameters validation

Testing objective

To assess the **design** and **operating effectiveness** of monitoring reports in identifying policies with frequent ownership changes with material payouts in accordance with predefined rules and parameters

Testing approach

Walkthrough interviews

With IT and Operations departments to **understand** the reporting logic:

- embedded parameters filters and thresholds

Conduct reperformance

Extract **raw transactional** data involving **policy ownership changes and payments** from January to June 2025 from source systems.

Data analytics

Use **spreadsheets** or **other computer software**

The reviewers are able to independently **filter out transactions** involving policy ownership changes and payouts

Data analytical techniques

Filtered out transactions on a **per policy** and **per policyholder** basis (e.g. using pivot table or applying formulae) according to the predefined rules and parameters.

To **validate** the report's **completeness** and **accuracy** and determine any **discrepancies**.

Extended reading: Conduct in focus – Special Supplement in September 2025

Extended reading: Conduct in focus – Special Supplement in September 2025

保險業監管局
Insurance Authority

CONDUCT IN FOCUS
Special Supplement
September 2025

Digitization of Conduct Monitoring and Controls

Issue 11 – Special Supplement
September 2025

Observations **on Common Shortcomings** in **Design and Implementation**

- Insufficient testing of system logic
- Inadequate Data Management
- Calibration of parameters

Areas of **Improvement**

https://www.ia.org.hk/en/legislative_framework/files/Eng_Conduct_in_Focus_Issue_11_September_2025_Special_Supplement.pdf

Thank You

(852) 3899 9983

(852) 3899 9993

enquiry@ia.org.hk

www.ia.org.hk

蓋世保鑑 Insurpedia