



# Anti-Money Laundering and Counter-Financing of Terrorism Webinar 2024

November 2024

# Disclaimer and Reminder

Where this presentation refers to certain aspects of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO) and the guidelines on anti-money laundering/ counter-financing of terrorism (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 or 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. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the SFC's prior written consent.

# Report on the Adoption of Regtech for Anti-Money Laundering and Counter-Financing of Terrorism

- 
- (1) Observations on the current state of Regtech adoption in the industry
  - (2) Common types of Regtech solutions adopted in major AML/CFT processes
  - (3) Responsible adoption of Regtech solutions in the AML/CFT processes
- 

## Speakers:

**Joyce Pang**

*Associate Director and Head of AML  
Intermediaries Supervision*

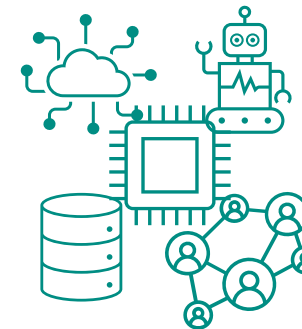
**Sharon Wong**

*Senior Manager  
Intermediaries Supervision*

# Background



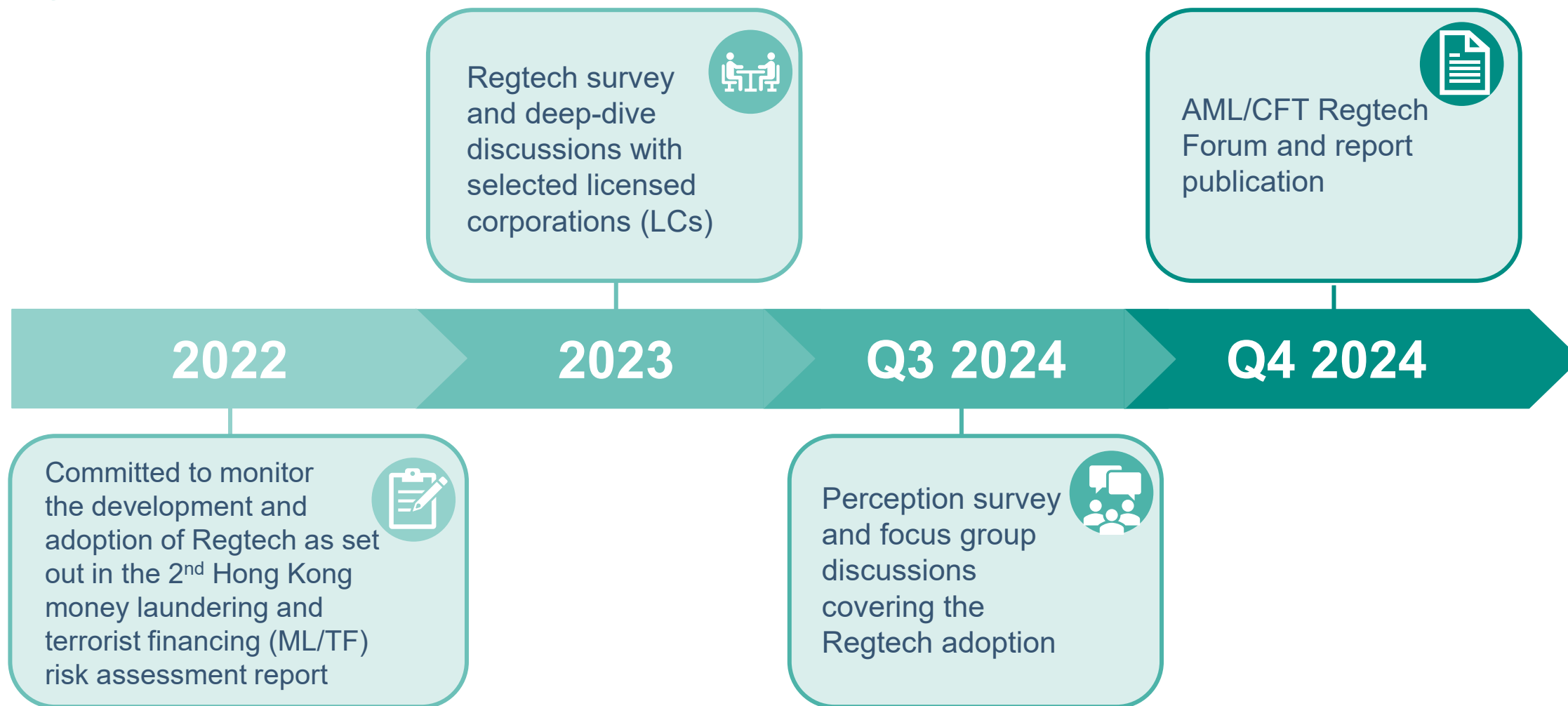
- **Financial crime** is getting **increasingly sophisticated** and **conventional manual approaches** in detecting and preventing money laundering and related predicate offences are becoming **less effective**
- **Increasing volume of data** that encompasses indicators of risk attributes, which often **go unnoticed** by **conventional monitoring methods**



In recent years, the Financial Action Task Force (FATF) has been:

- actively promoting the awareness of **leveraging new and existing technology-based solutions** for AML/CFT processes
- encouraging the **responsible adoption** of Regtech to ensure the effective implementation of AML/CFT measures

# The SFC's initiatives to monitor the development and progress of Regtech adoption



# AML/CFT Regtech Forum 2024

More than 300 participants – including government officials, industry representatives and experts – attended **SFC AML/CFT Regtech Forum** on 4 November 2024.



“It is **more affordable than you think**, especially **compared to the heavy cost of overlooking** money laundering risks.”



“As we move forward, let us **embrace the potential** of technology while ensuring that our regulatory frameworks **keep pace with the innovation.**”

# AML/CFT Regtech Forum 2024



“The transformative power of Regtech in analysing vast amounts of data enables the **prompt and effective detection and management of risks** related to ML/TF.”

“We do not have a choice but to do name screening and fulfil other regulatory requirements effectively including corroborating customers’ information. That’s why we have to **use technology**.”

“It should be the **senior management** leading from the top to **set the vision** and **combine the efforts of both talent and technologies** in order to combat sophisticated crimes.”

# AML/CFT Regtech Forum 2024



“We can see different level of ML/TF risks immersed throughout the lifecycle of a customer from onboarding, trading to exiting. Use of technologies can really help us **lower the regulatory burden** in complying with different requirements.”

“For institutions with online business model, it is a must to deploy Regtech, just a matter of **intensity and areas of focus.**”

“**Data quality** is the key to building an effective Regtech tool for analysing and identifying emerging risks.”



# AML/CFT Regtech Forum 2024



“Use of Regtech does not only help in complying regulatory requirements, but also fostering a more **efficient operational flow** and **enhancing the customer onboarding journey and experience.**”

“Building a one-stop solution for different modules of AML requirements may seem to need more resources than maintaining siloed systems, but the **enhanced efficiency in collaborating all data sources** in one click would speak for itself.”

“There is no perfect Regtech solution and every system has its own limitations. While we are well aware of the limitations, there are always ways to **overcome** them which should not keep us away from **embracing innovation and adopting technologies.**”

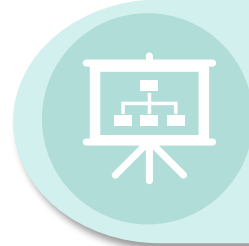
# Report on the adoption of Regtech for AML/CFT

The SFC issued a [report](#) on 4 November 2024 which aims to encourage the responsible and broader adoption of Regtech to assist LCs in complying with AML/CFT requirements.

The report includes sharing of:



observations on the current state of Regtech adoption



illustrative use cases of common types of Regtech solutions



responsible adoption of Regtech solutions in the AML/CFT processes

# Regtech survey results

In mid-2023, the SFC conducted a comprehensive Regtech survey on 50 selected LCs.



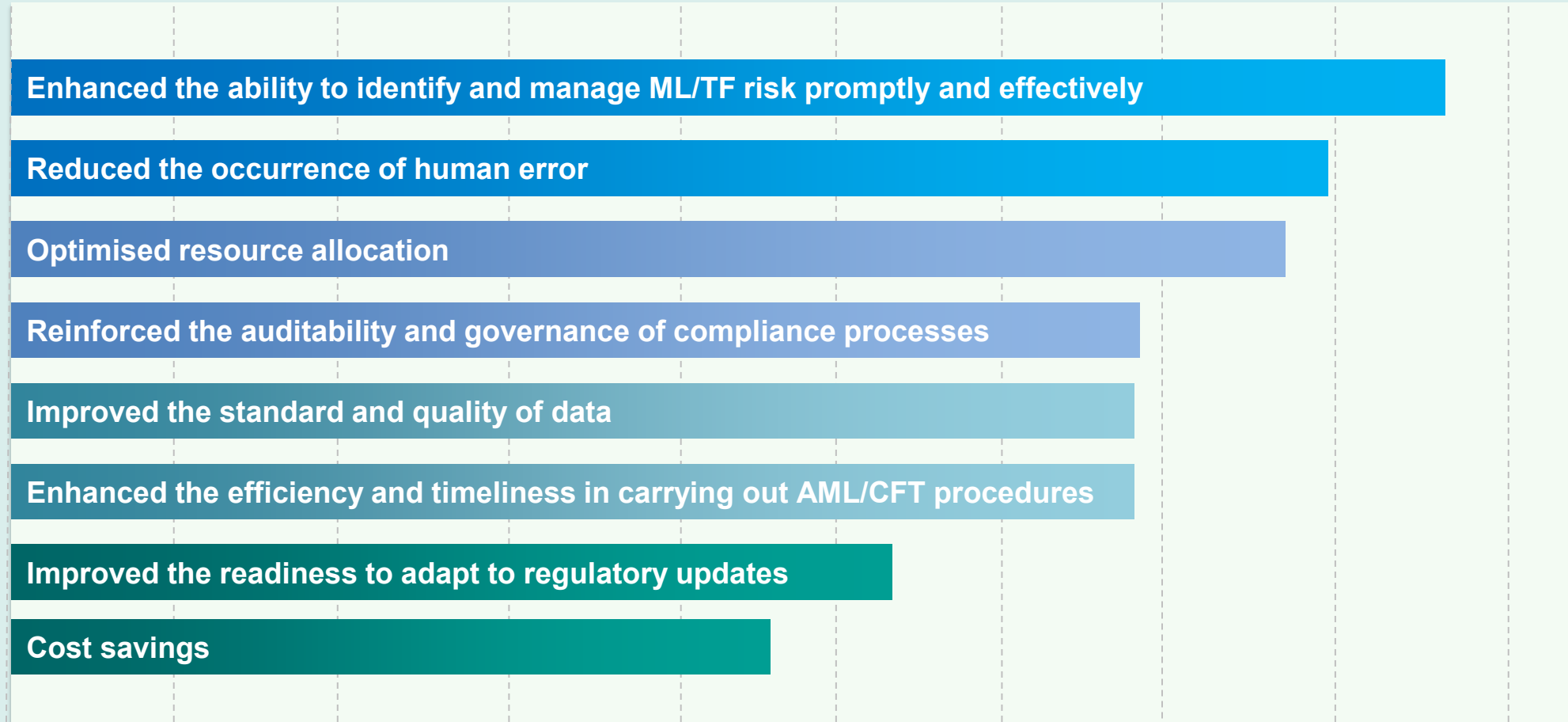
The survey aimed to gauge the LCs' adoption status of Regtech in the AML/CFT processes and gain a deeper understanding of their adoption process in the following aspects:

- the adoption status and features of the Regtech solutions in major AML/CFT processes;
- the benefits and challenges of Regtech adoption; and
- the development, implementation and ongoing monitoring of the Regtech solutions.

# Regtech survey results

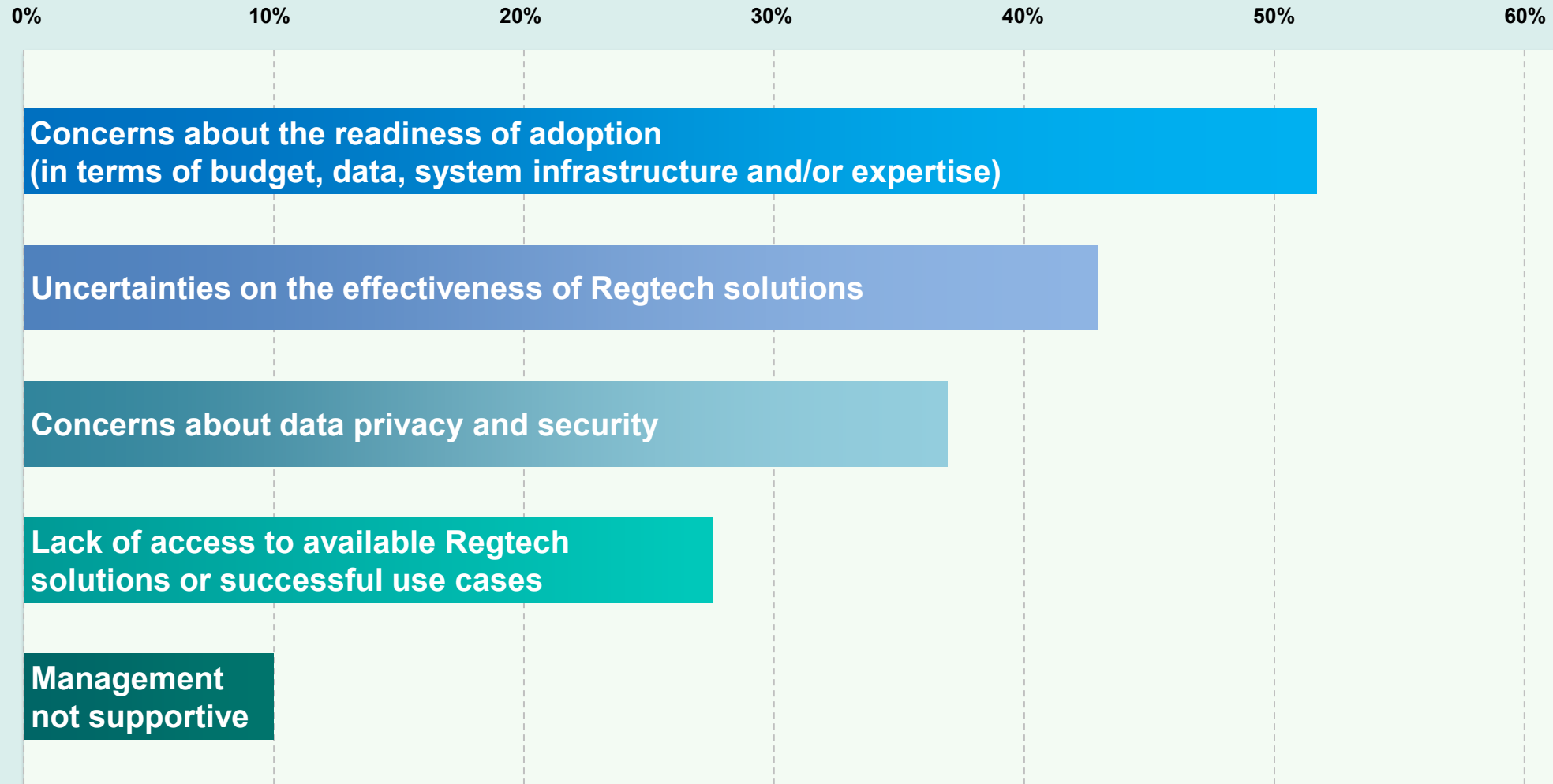
## Benefits of Regtech adoption

0% 10% 20% 30% 40% 50% 60% 70% 80% 90%



# Regtech survey results

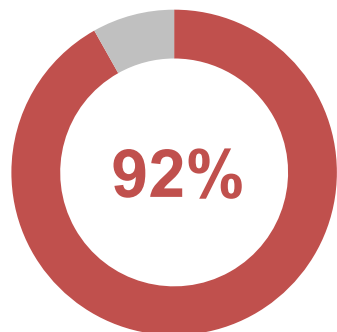
## Challenges of Regtech adoption



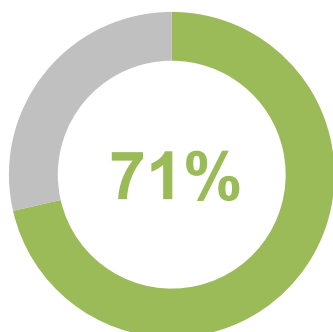
# Regtech survey results

Regtech adoption rate in major AML/CFT processes

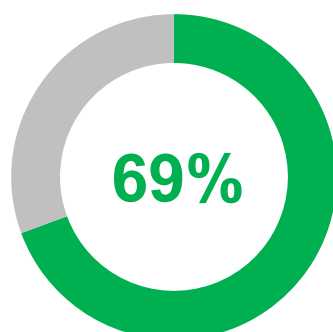
Name  
screening



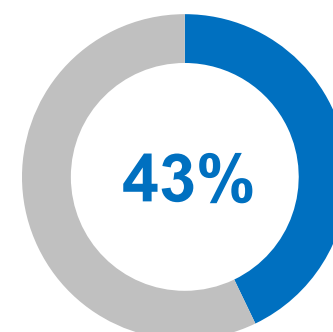
Customer due  
diligence (CDD)



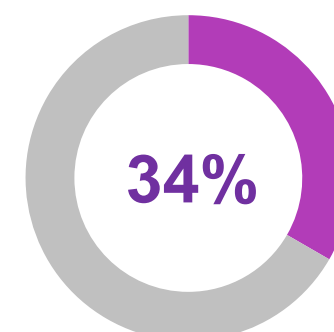
Transaction  
monitoring



Management  
information  
reporting



Third-party  
deposit  
identification and  
due diligence



# Report on the Adoption of Regtech for Anti-Money Laundering and Counter-Financing of Terrorism

---

- (1) Observations on the current state of Regtech adoption in the industry
  - (2) Common types of Regtech solutions adopted in major AML/CFT processes**
  - (3) Responsible adoption of Regtech solutions in the AML/CFT processes
-

# Common types of Regtech solutions adopted in name screening



92%

Adoption rate



80%

of the respondents have adopted Regtech solutions in this area for 5 years or more



## Top three common functions:

- identifying names with alteration
- auto-screening of existing customers and any beneficial owners of customers against new and any updated designations
- advanced filtering to reduce false-positive screening alerts



67%

of the respondents took less than a year from decision to implementation of Regtech solutions



**More mature** compared to the other AML/CFT processes



LCs generally recognised that these solutions can **significantly enhanced efficiency and effectiveness** by reallocating resources to review screening alerts with higher risks

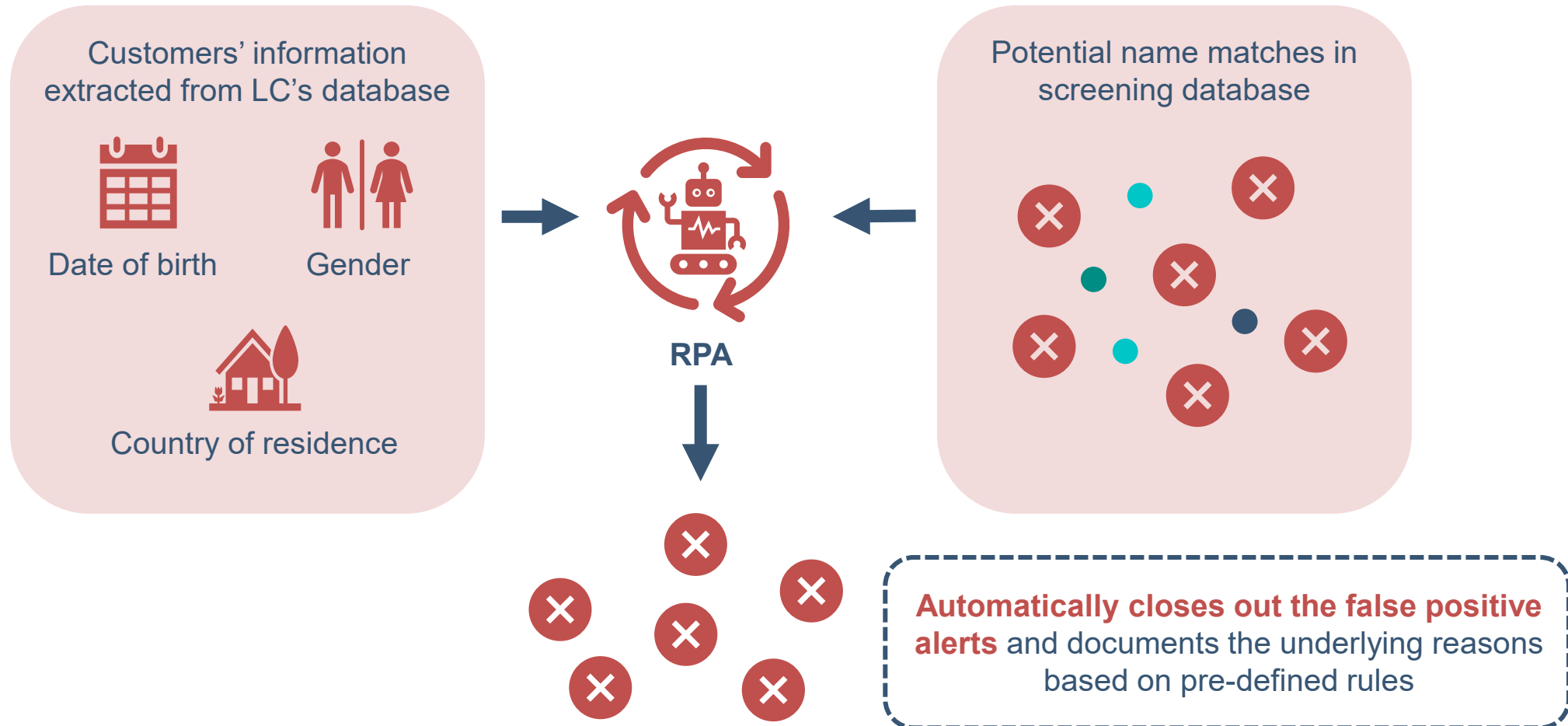


Some LCs adopted advanced functions such as **applying machine learning** to evaluate the likelihood of an alert to be false positive by considering the customer profile



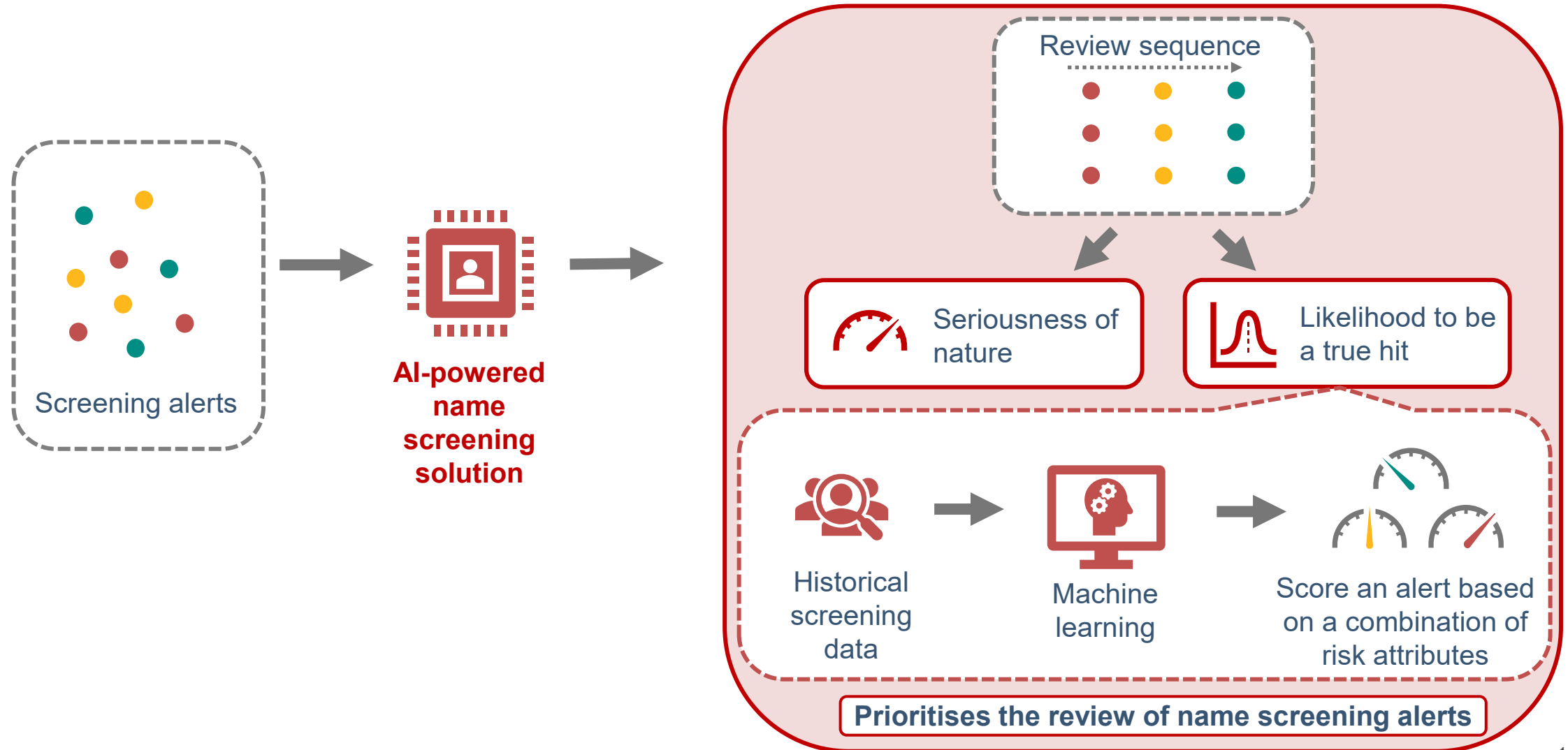
# Common types of Regtech solutions adopted in name screening

Illustrative use case: Implementing robotic process automation (RPA) which automatically closes out alerts with mismatched information



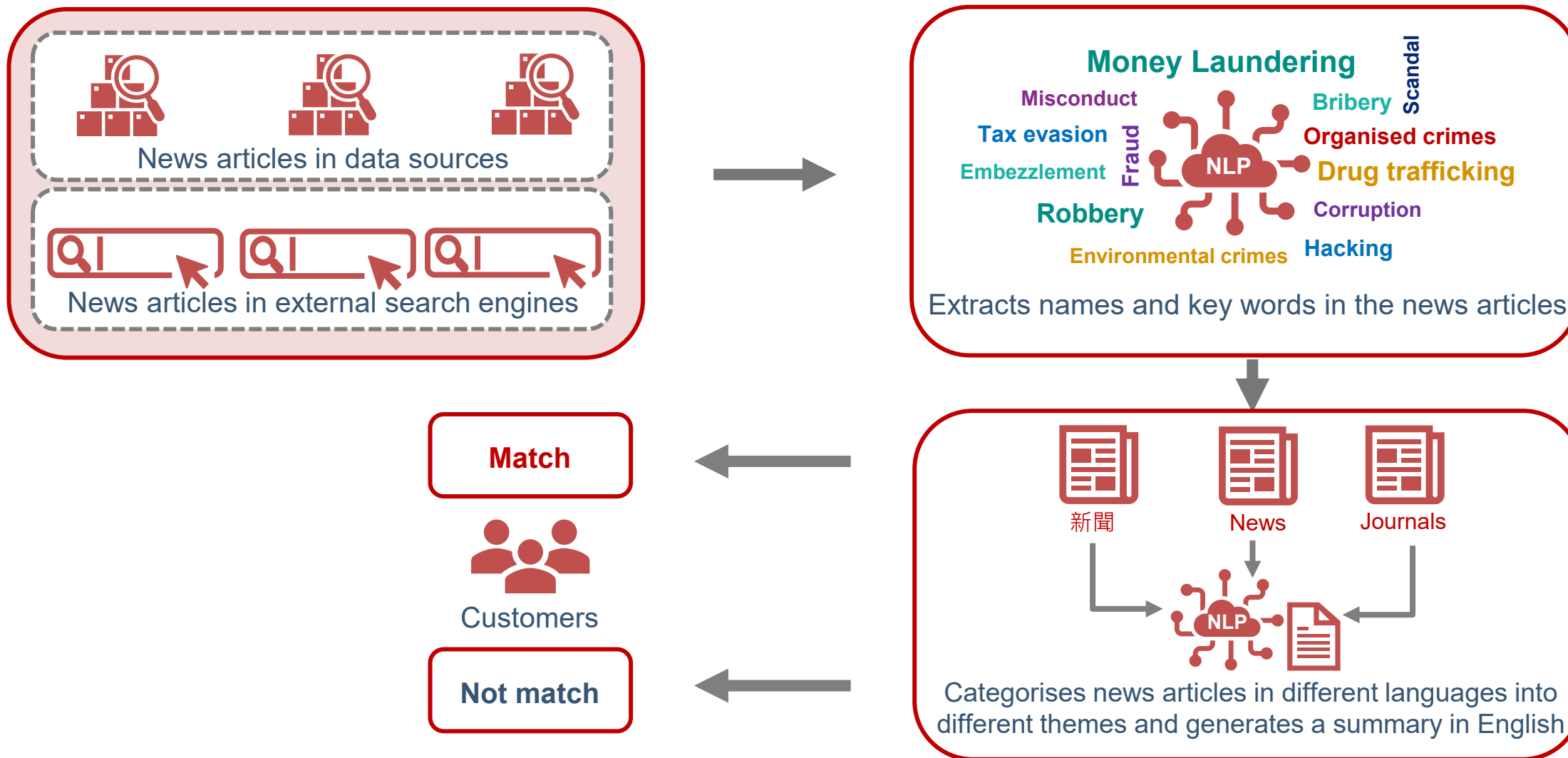
# Common types of Regtech solutions adopted in name screening

Illustrative use case: Artificial intelligence (AI) powered name screening solution



# Common types of Regtech solutions adopted in name screening

Illustrative use case: Natural language processing (NLP) engine in adverse media screening solution



# Common types of Regtech solutions adopted in CDD



71%

Adoption rate



71%

of the respondents' solutions can facilitate onboarding of individual customers



83%

of the respondents' solutions can facilitate customer risk assessment (CRA)



86%

of the respondents' solutions can facilitate CDD and ongoing monitoring measures



69%

of the respondents took less than a year from decision to implementation of the Regtech solutions



LCs commonly start adopting Regtech solutions at the **onboarding stage**



Some surveyed LCs indicated that their Regtech solutions have assisted in **verifying or authenticating a customer's identity**



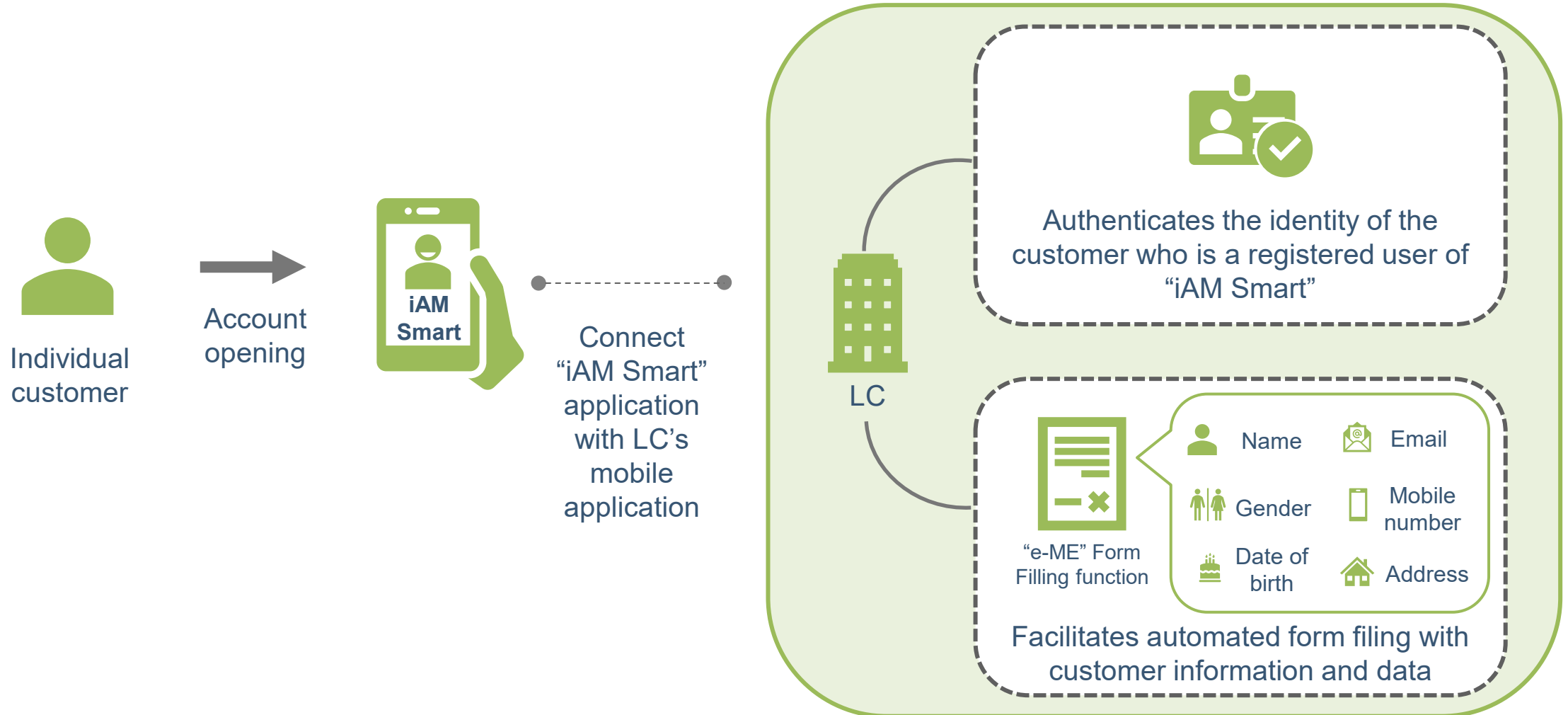
Some LCs employed analytics solutions to facilitate **ongoing CDD reviews** or detect situation which warrant **trigger event-driven reviews**



Some LCs adopted Regtech solutions for **customer risk assessment** which help analyse customer data more comprehensively and accurately

# Common types of Regtech solutions adopted in CDD

Illustrative use case: Identity verification and automated form filling through adoption of “iAM Smart”



# Common types of Regtech solutions adopted in transaction monitoring



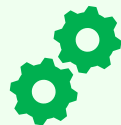
69%

Adoption rate



65%

of the respondents took around 6 to 24 months from decision to implementation of the Regtech solutions



## Top three common functions:

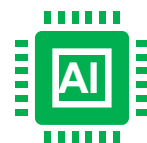
- use of pre-defined scenarios and rules to generate transaction monitoring alerts
- use of case management tool to document and track the workflow of transaction monitoring alerts handling
- triage the transaction monitoring alerts to be reviewed and/or investigated according to its handling priority



Most surveyed LCs adopted Regtech solutions to generate alerts of potential unusual or suspicious transactions based on **pre-defined rules and scenarios**



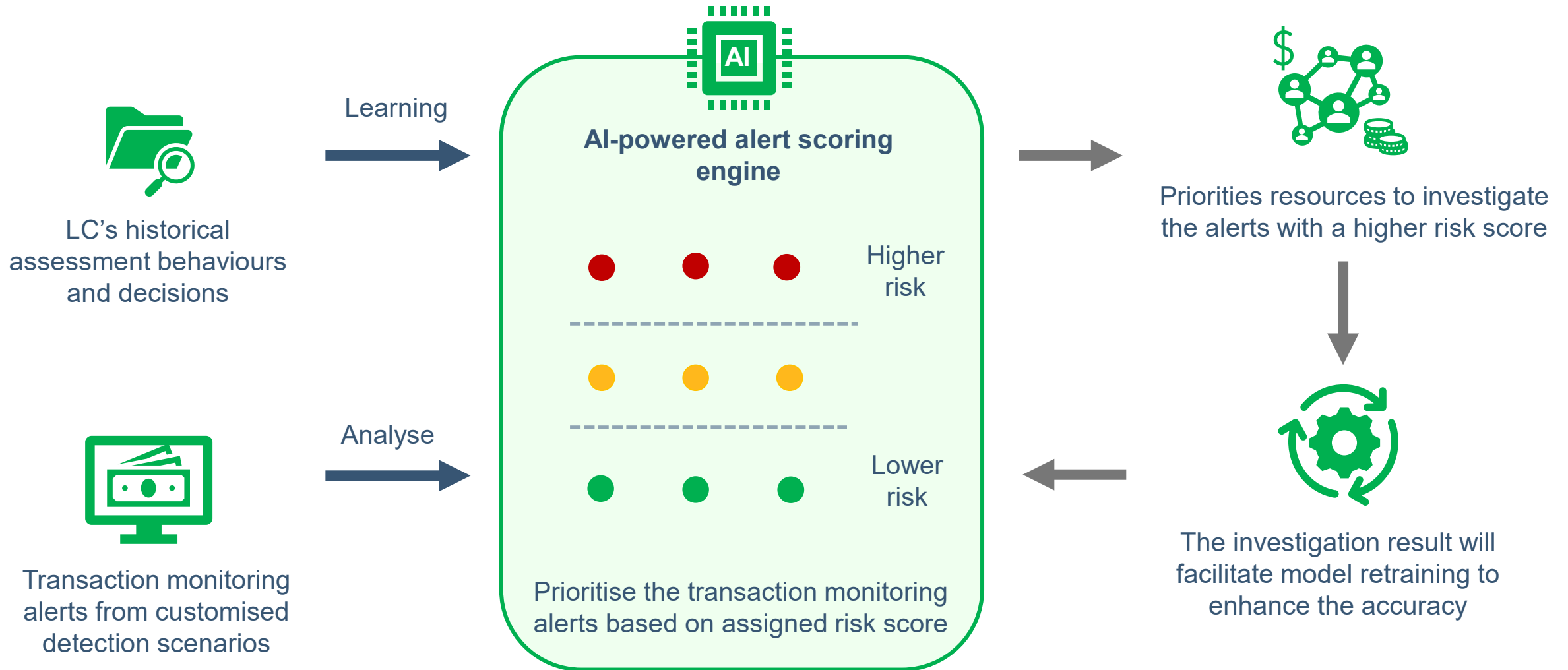
Some surveyed LCs have **started adopting more advanced underlying technologies**, eg, AI in their transaction monitoring process



Some LCs have **adopted other AI features**, for example, to prioritise alerts based on their risk score and filter out false positive alerts

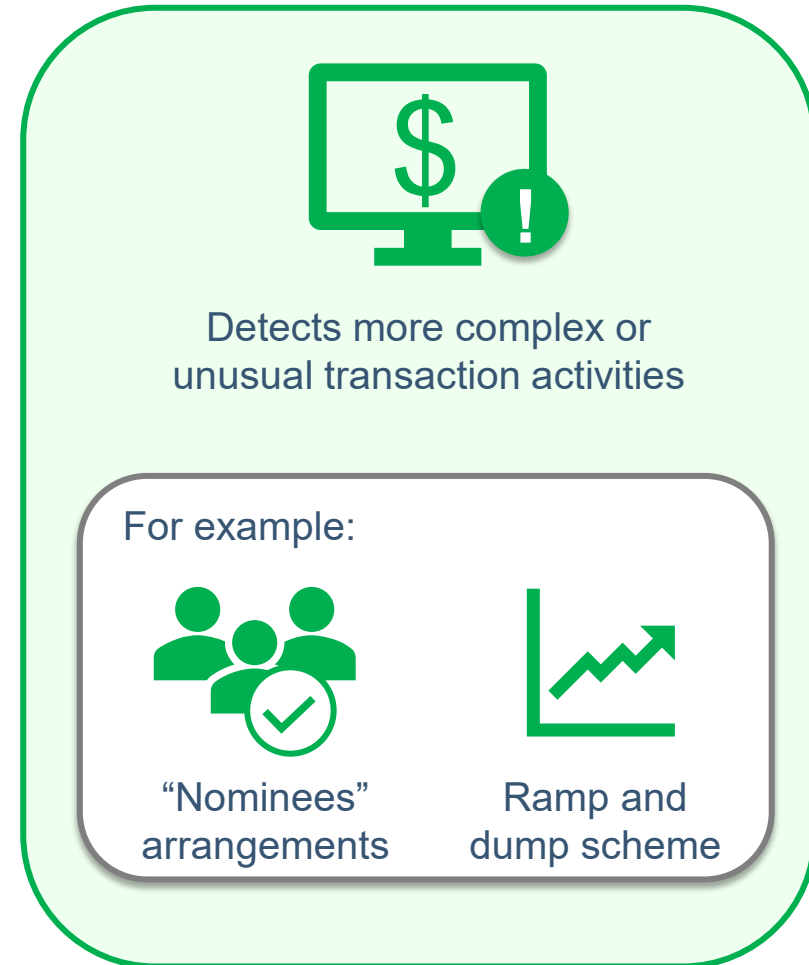
# Common types of Regtech solutions adopted in transaction monitoring

Illustrative use case: Transaction monitoring solution with an AI-powered alert scoring engine



# Common types of Regtech solutions adopted in transaction monitoring

Illustrative use case: Use of network analytics for transaction monitoring





# Common types of Regtech solutions adopted in management information reporting



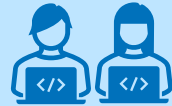
43%

Adoption rate



71%

of the respondents' solutions can facilitate ML/TF risk metrics generation for reporting purposes



95%

of the respondents' solutions are either developed by in-house development team or jointly developed with external development team



71%

of the respondents took less than a year from decision to implementation of Regtech solutions

Some LCs recognise the benefits of adopting Regtech solutions, such as data analytics dashboard:



to facilitate the **analysis, understanding, and managing of AML/CFT compliance risk holistically**



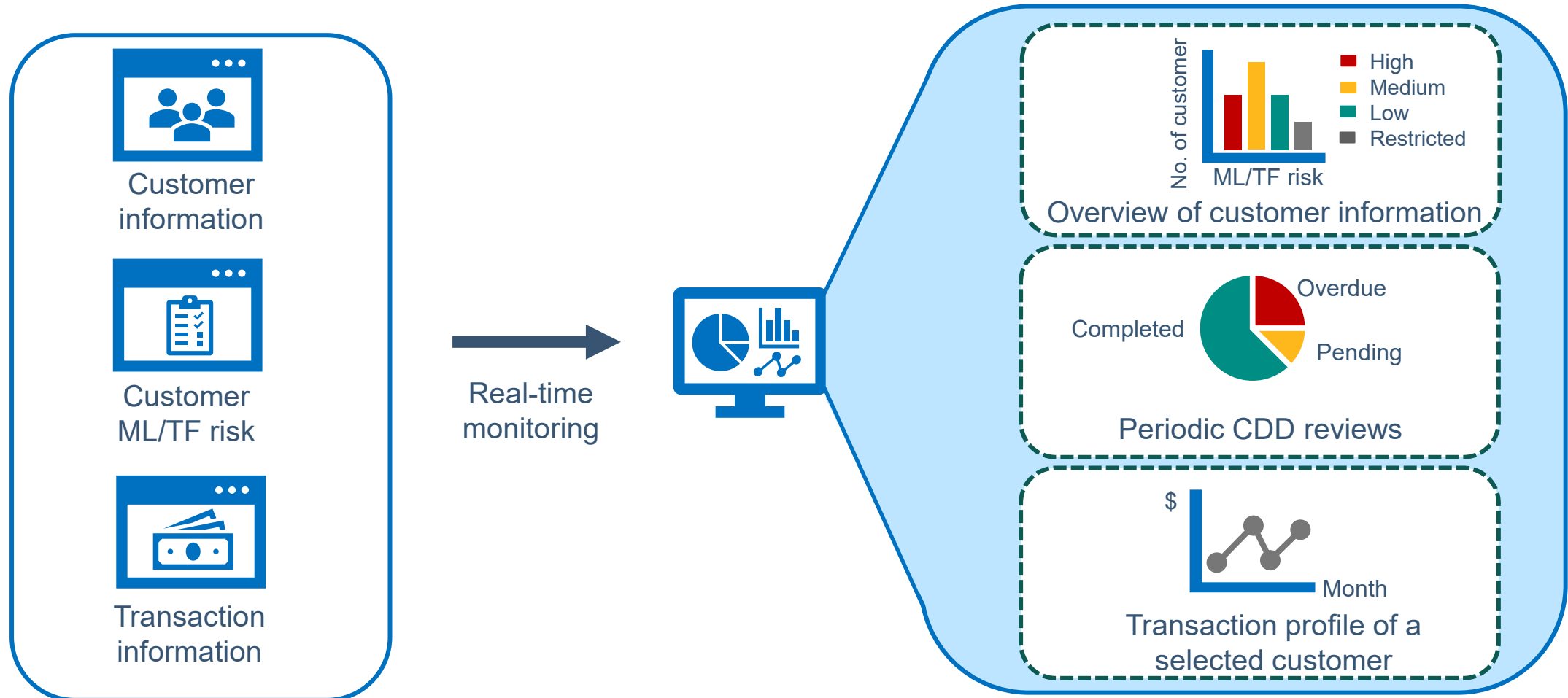
**saves time** by eliminating the preparation of multiple management information reports



to facilitate LC's performance of **institutional risk assessment and compilation of statutory returns** such as the Business and Risk Management Questionnaire

# Common types of Regtech solutions adopted in management information reporting

Illustrative use case: Management information system using a dynamic dashboard with real-time data feed



# Common types of Regtech solutions adopted in third-party deposit identification and due diligence



34%

Adoption rate\*

*\*Excluding eight surveyed LCs which indicated that they do not handle any fund deposits and withdrawals for their customers*



71%

of the respondents took less than a year from decision to implementation of Regtech solutions



86%

of the respondents' solutions are either developed by in-house development team or jointly developed with external development team



Relatively less mature primarily because the AML/CFT requirements on third-party deposits and payments are **unique to the securities sector** and **only came into place in 2019**



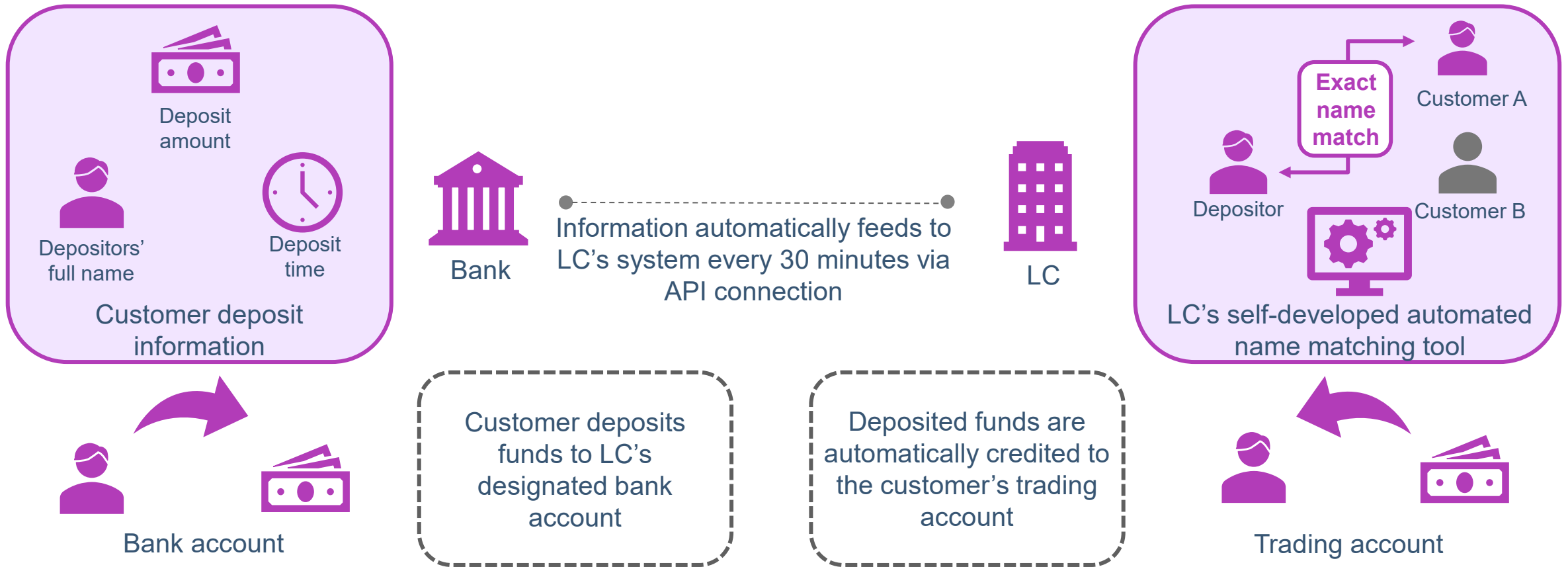
Some larger brokerages have chosen to implement Regtech solutions to **automate the verification of deposit sources**



Some LCs have adopted Regtech solutions to help ensure that the **required due diligence measures on third-party deposits and payments are conducted in a timely manner and with proper approval**

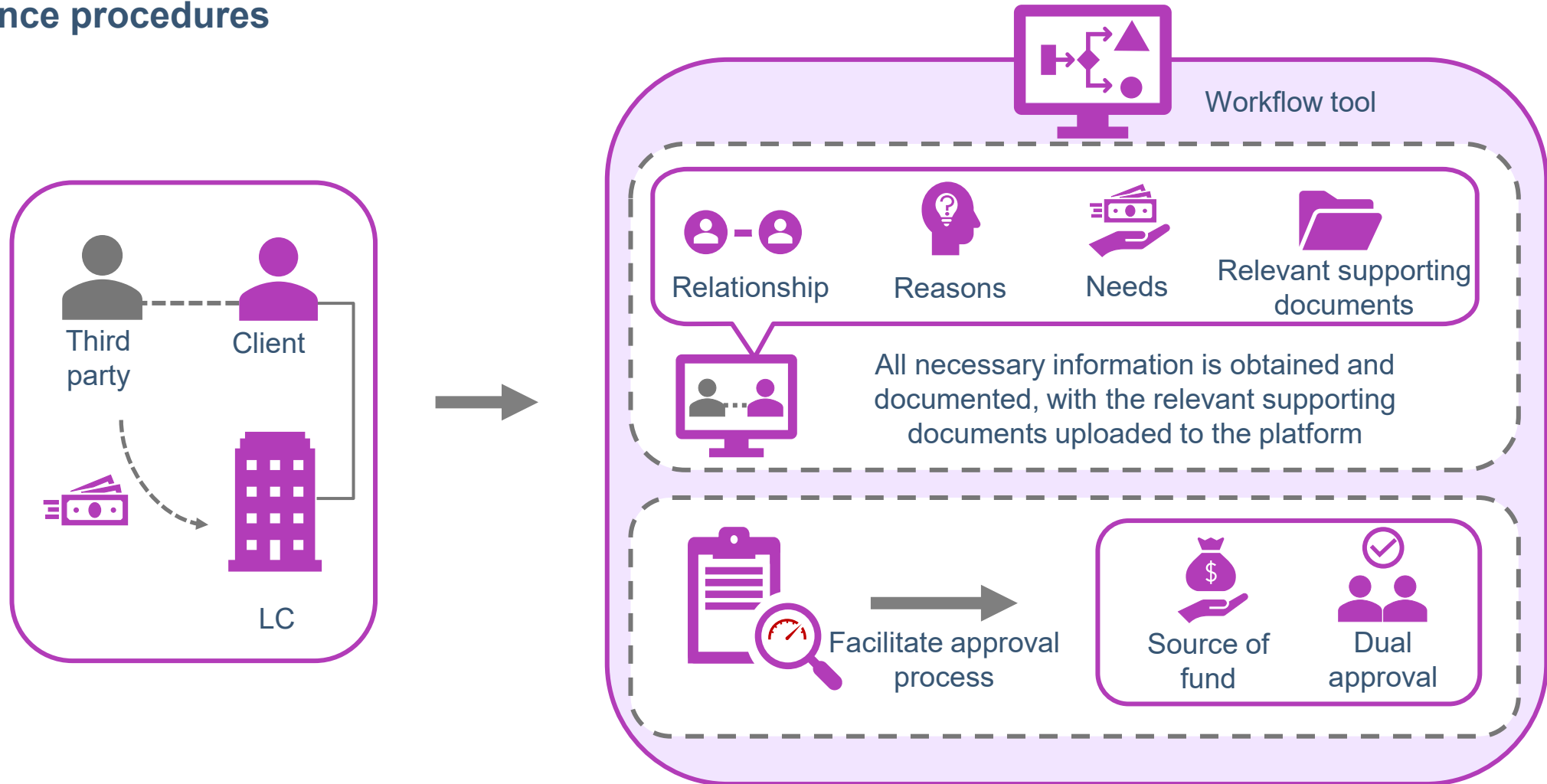
# Common types of Regtech solutions adopted in third-party deposit identification and due diligence

Illustrative use case: Use of API and automated name screening tool to facilitate the identification of third-party deposit



# Common types of Regtech solutions adopted in third-party deposit identification and due diligence

Illustrative use case: Using workflow tool for the performance of third-party deposit due diligence procedures



# Report on the Adoption of Regtech for Anti-Money Laundering and Counter-Financing of Terrorism

- 
- (1) Observations on the current state of Regtech adoption in the industry

---

  - (2) Common types of Regtech solutions adopted in major AML/CFT processes

---

  - (3) Responsible adoption of Regtech solutions in the AML/CFT processes**

---

# Responsible adoption of Regtech solutions in the AML/CFT processes

**Governance and accountability**

**1**



**2 Ongoing monitoring of Regtech solutions**



**Managing risks posed by external vendors**

**4**



**3 Data protection and cybersecurity**



# Responsible adoption of Regtech solutions in the AML/CFT processes



## Governance and accountability



The **senior management** of an LC is responsible for implementing effective AML/CFT policies, procedures and controls



To ensure that any Regtech solutions adopted are subject to proper governance and oversight, the **policies and procedures** should include:

- conducting proper **due diligence and testing** on the Regtech solutions;
- ensuring the Regtech solutions are subject to **regular review**; and
- ensuring the parameters, thresholds, algorithms and system logics, adopted in the Regtech solutions are **properly documented** and subject to appropriate level of **approval by senior management**



# Responsible adoption of Regtech solutions in the AML/CFT processes



## Ongoing monitoring of Regtech solutions



Implement a solution that is **proportionate to their own needs, capabilities and unique circumstances** and avoid adopting a plug-and-play approach without properly evaluating the performance of the Regtech solutions on an ongoing basis



Have a **demonstrable and thorough understanding** of how the Regtech solutions work



The adequacy, appropriateness and effectiveness of the parameters and thresholds should be subject to **independent validation and ongoing monitoring**

# Responsible adoption of Regtech solutions in the AML/CFT processes



## Data protection and cybersecurity



Ensure that the customer and transaction data, systems and networks are **subject to adequate and appropriate protection**



Undertake **measures to safeguard personal data** from unauthorised access, use or disclosure



Establish **cybersecurity measures** such as encryption, firewalls and access controls to safeguard the computer systems and networks from cybercrime and cyberattacks

# Responsible adoption of Regtech solutions in the AML/CFT processes



## Managing risks posed by external vendors



Be mindful of the **risks posed by the external vendor** and **implement appropriate measures** to manage and mitigate any potential risks



Exercise **due skill, care and diligence** in the selection of the external vendor

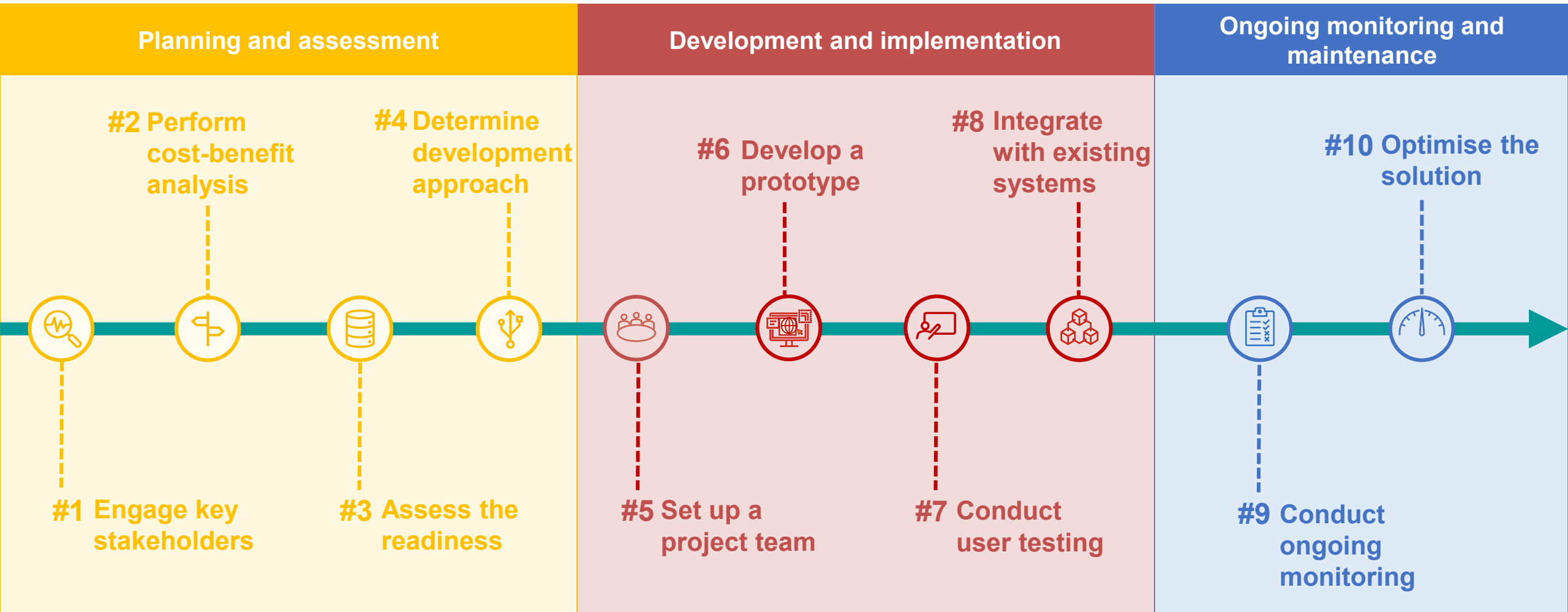


Due considerations should be given to the external vendor's controls related to **data governance and protection as well as cybersecurity measures**



Establish **appropriate contingency plans** to ensure their AML/CFT systems and controls remain resilient in the event of disruption of the Regtech solutions

# Regtech adoption roadmap



# Sharing of supervisory observations related to AML/CFT

---

(1) Deficiencies and inadequacies found in LCs' AML/CFT systems and controls

---

(2) Case examples

---

**Speaker:**

**Edward Lam**

*Manager*

*Intermediaries Supervision*

# Customer due diligence

## Example 1 - Customer not physically present for identification purpose

An LC accepted establishing business relationship via online channels by using a designated bank account in Hong Kong or overseas.



The LC failed to:

- refer to the **list of eligible jurisdictions** on the SFC website to ascertain the designated bank account used by its overseas customers is maintained with a bank which is supervised by a banking regulator in an eligible jurisdiction; and
- take reasonable measures to **ascertain the designated bank account is in the customer's name.**

# Customer due diligence

## Example 2 – Application of simplified customer due diligence (SDD)

An LC applied SDD measures when establishing business relationship with a customer, which is an investment vehicle.



The LC failed to take appropriate steps to ensure that the customer met the eligibility criteria for applying SDD measures, which include:

- ascertaining that the **person responsible for carrying out the CDD measures** falls within any of the **categories of institution** set out in section 4(3)(d) of Schedule 2 to the AMLO; and
- satisfying that the investment vehicle had ensured that there were **reliable systems and controls** in place to **conduct CDD on the underlying investors**.

# Customer due diligence

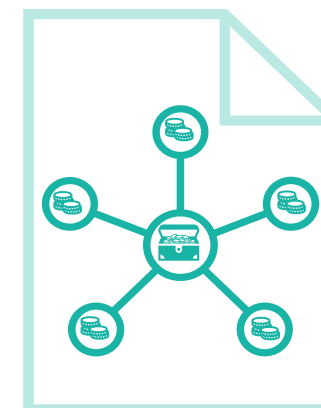
## Example 3 - Special requirements in high-risk situations

An LC adopted enhanced due diligence measures for high-risk customers by:

- requesting them to provide their source of wealth and source of funds information in the account opening form; and
- conducting public domain search on the customers and their beneficial owners to corroborate the information.



However, in practice, the LC only relied on limited information as obtained in the account opening form for establishing the source of wealth and source of funds for its high-risk customers, eg, salary and investment gains, without taking any reasonable measures to **further corroborate the information obtained** or **taking additional measures** to mitigate the risk of ML/TF.





# Customer due diligence

## Example 4 - Treatment of former non-Hong Kong politically exposed persons (PEP)

An LC identified a customer as a former non-Hong Kong PEP. In determining whether the customer is no longer presented a high risk of ML/TF, the LC only considered the fact that the customer had stepped down from the position that held as a non-Hong Kong PEP.



The LC failed to conduct an appropriate assessment of the ML/TF risk associated with the previous PEP status taking into account various risk factors, including but not limited to:

- the **level of (informal) influence** that the individual could still exercise;
- the **seniority of the position** that the individual held as a non-Hong Kong PEP; and
- whether the individual's **previous and current functions** are **linked** in any way.

# Ongoing monitoring

## Example 5 - Timeliness of ongoing customer due diligence

An LC conducted annual CDD review on its high ML/TF risk customers and would suspend the customer's account if the review is overdue.



The LC failed to:

- initiate the **CDD review** of its high ML/TF risk customers **on or before the due date**; and
- **suspend** the customer's account in accordance with its internal policy.



# Screening for PEPs, terrorist suspects and designated parties

## Example 6 - Effectiveness of screening mechanism

An LC adopted an automated screening solution to perform name screening of its customers, which covered sanctions, PEPs and negative news, during customer onboarding and thereafter on a daily basis.



The LC failed to:

- implement measures to **screen** all new and any updated designations against **beneficial owners** of the customers, and extend the screening requirements to **connected parties** and **person purporting to act** on behalf of the customers using a risk-based approach;
- review the **effectiveness** of the **rules and matching algorithm** to prevent possible genuine matches being overlooked;
- take appropriate measures to **ensure the completeness and accuracy** of the **screening database** maintained for sanctions screening; and
- institute appropriate measures and **provide guidance to the staff** for the handling of screening alerts and require **documentation** of the justifications.

# Transaction monitoring

## Example 7 - Adequacy and effectiveness of transaction monitoring systems and controls

An LC relied on its staff to conduct pre-transaction monitoring which focused on the identification of large fund transactions, and post-transaction monitoring on selected types of transactions.



The LC failed to:

- justify the **adequacy** and **effectiveness** of the **thresholds** adopted for the transaction monitoring system;
- examine the **background** and **purposes** of the transactions, nor **make enquiries** to or **obtain additional CDD information** from the customer to evaluate if there were any grounds for suspicion; and
- have adequate processes in place to **monitor different types** of transactions.

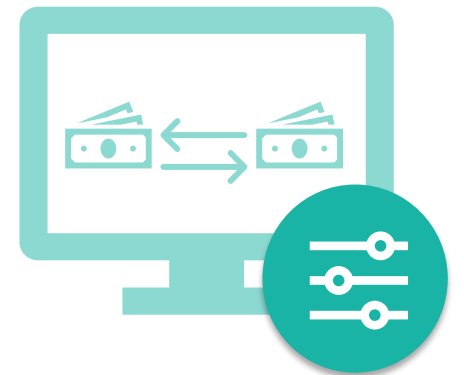
# Transaction monitoring

## Example 8 - Effectiveness of the transaction monitoring system

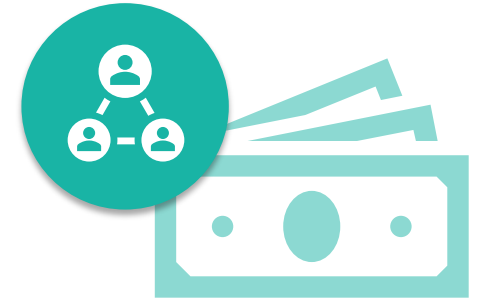
An LC adopted an automated transaction monitoring system for monitoring and detecting unusual transaction patterns or behaviours based on various transaction monitoring scenarios. The transaction monitoring scenarios and thresholds adopted are subject to review by an independent consultant on a regular basis and are adjusted based on the recommendation.



The LC relied on the independent consultant's conclusion and adopted all recommended scenarios and thresholds without taking steps to **understand how the recommended thresholds were derived** or **evaluate the reasonableness of the proposed adjustments** to ensure that they were appropriate to its operations and context.



# Third-party deposits and payments



## Example 9 - Handling of third-party payments

An LC, which is an asset manager of an investment fund, paid certain amount of distribution to a third party as instructed by the fund investor.



The LC failed to conduct relevant **due diligence process** for **assessing whether third-party payments** proposed by the fund investor meet the evaluation criteria for acceptance.

## Example 10 - Handling of third-party deposits

An LC accepted a third-party deposit from a licensed money lender to its customer which was declared as a rebate of interest under the memoranda of loan facility.



The LC failed to **implement effective controls** to ensure third-party deposits could only be accepted under **exceptional and legitimate circumstances**.

# Third-party deposits and payments

## Example 11 - Standing approval for third-party deposits and payments

An LC granted standing approvals for accepting deposits and/or payments from or to a particular third party after assessing the risk and reasonableness of the third-party arrangement.



The LC failed to:

- **critically evaluate** the appropriateness of the standing approval and the need for such arrangement to justify they are **reasonably in line** with the customer's **profile and normal commercial practices**; and
- **review** the standing approval periodically or upon trigger events to ensure that it **remains appropriate**.

# Sharing of supervisory observations related to AML/CFT

---

(1) Deficiencies and inadequacies found in LCs' AML/CFT systems and controls

---

**(2) Case examples**

---



# Case example 1



Failure to perform adequate **due diligence on the customer supplied systems (CSSs)**, and assess and manage the **associated ML/TF and other risks**



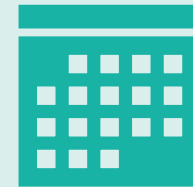
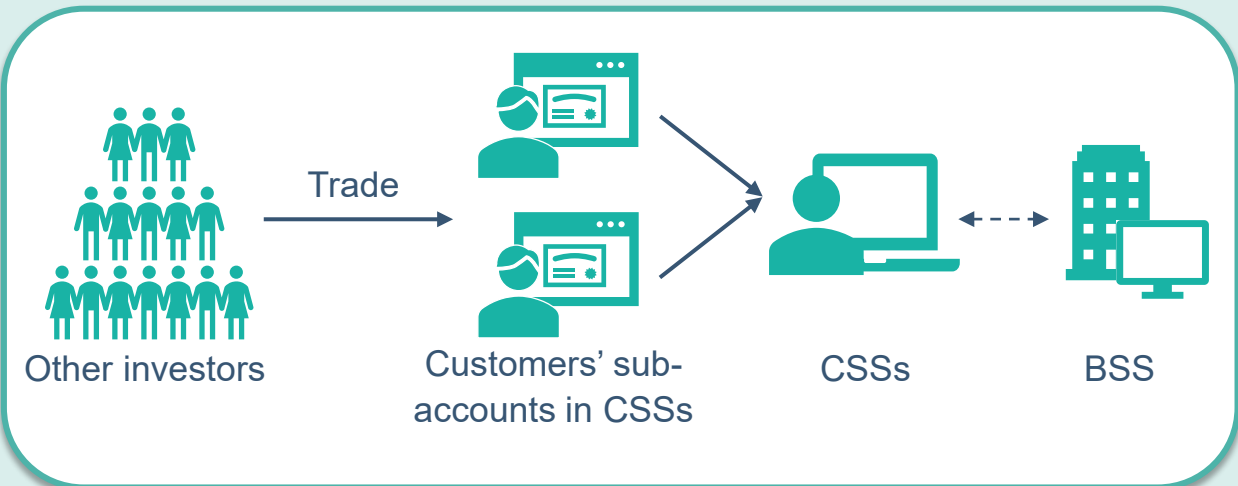
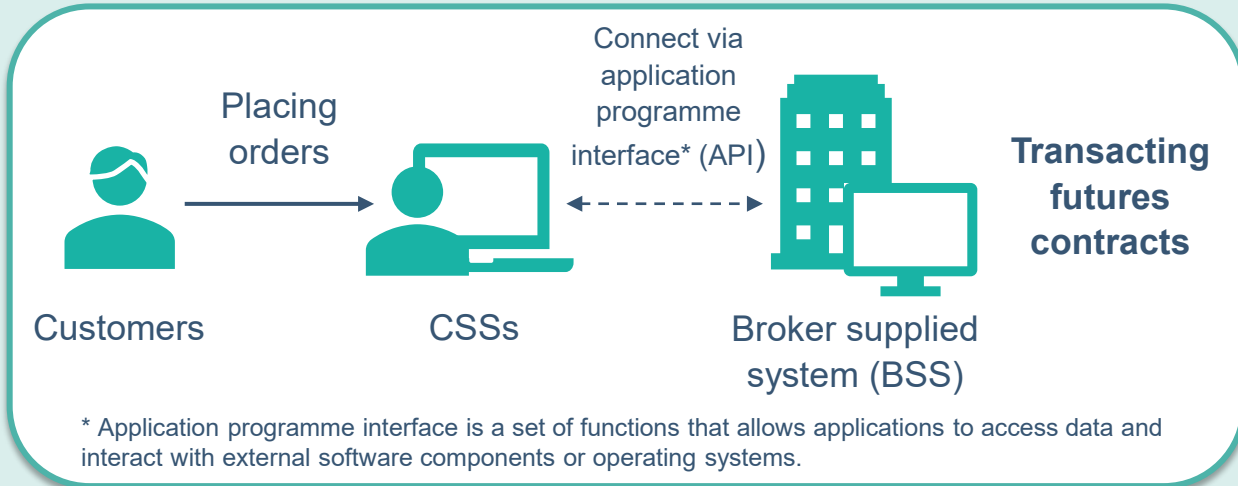
Failure to conduct **proper enquiries** on customer deposits which were **incommensurate with the customer's financial profiles** and implement adequate systems and controls on **monitoring and assessing large, unusual or suspicious customer deposits**



Failure to maintain **effective ongoing monitoring system** to detect and assess suspicious trading patterns in customer accounts

# Case example 1

## Inadequate due diligence on CSSs



Between **December 2016** and **March 2019**

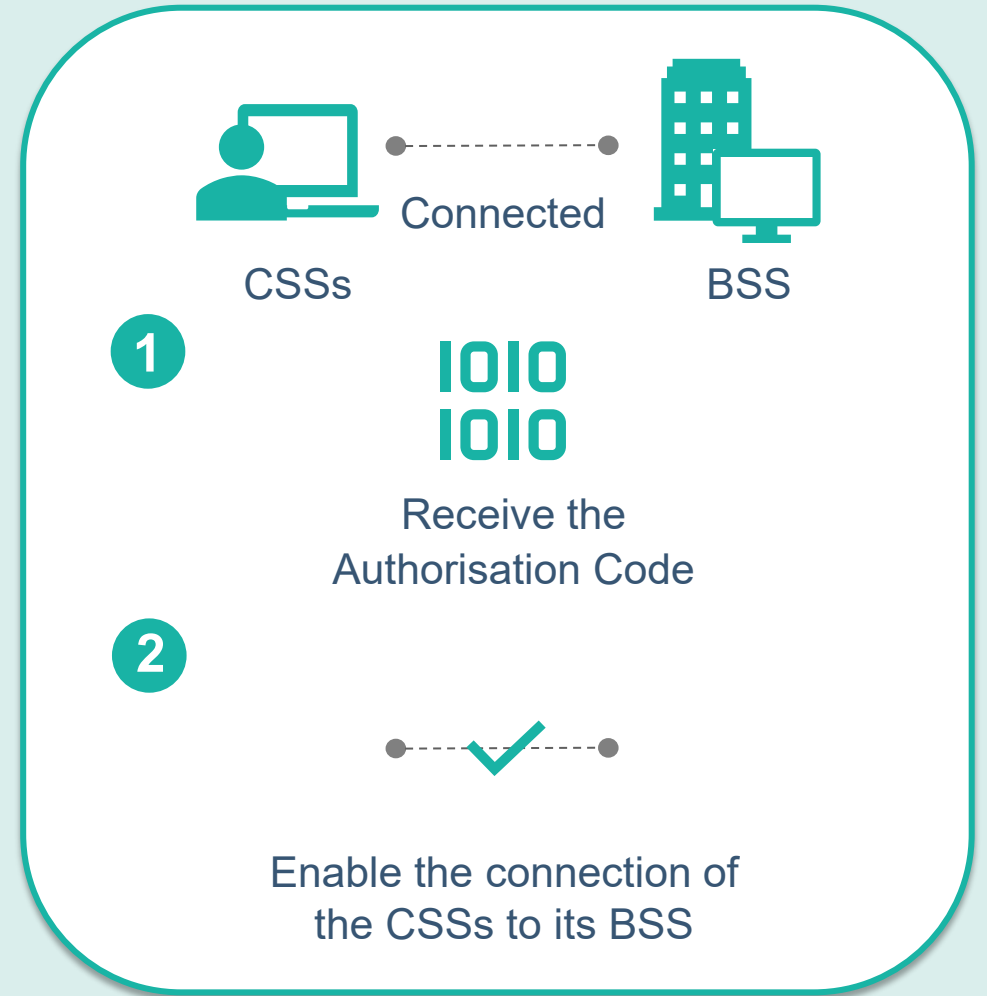
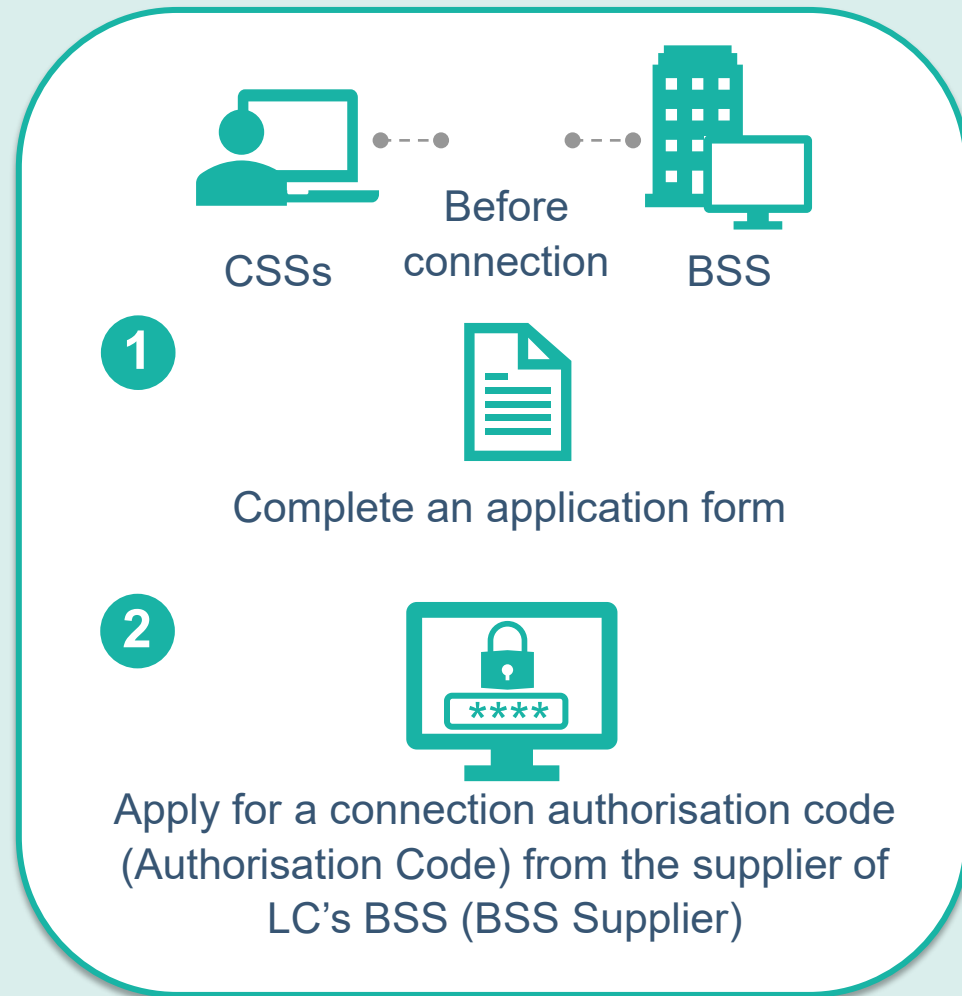
Permitted **more than 80**  **customers** to use their designated CSSs for placing order



**> 98%** of the total trading volume of all customers in the LC

# Case example 1

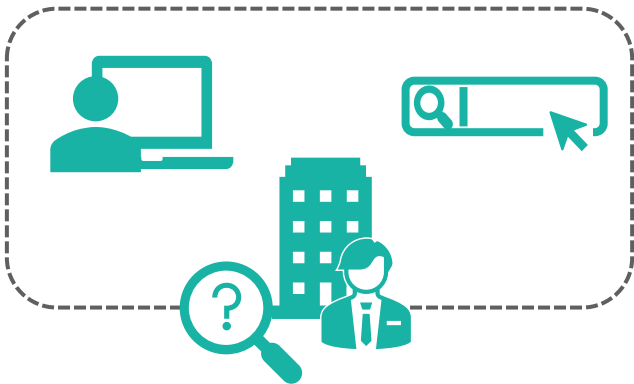
## Inadequate due diligence on CSSs



# Case example 1

## Inadequate due diligence on CSSs

The LC did not perform due diligence or testing on the CSSs used by its customers:



**No supporting evidence** to show the checks or tests performed by the staff member on the CSSs



The LC approved the customers' application forms **based solely on the BSS Supplier issuing the Authorisation Code**



The LC relied on the **BSS Supplier to conduct due diligence** on the CSSs

# Case example 1

## Inadequate due diligence on CSSs



- ✗ The features and functions of the CSSs
- ✗ Proper control over the use of CSSs by LC's customers



The LC was **not in a position to properly assess the ML/TF and other risks associated** with the use of the CSSs and implement appropriate measures and controls to mitigate and manage such risks





The LC has **exposed itself to the risks of improper conduct** such as unlicensed activities, money laundering, nominee account arrangement and unauthorised access to customer accounts

# Case example 1

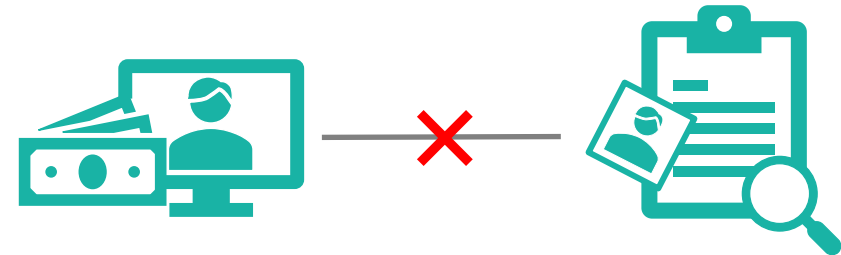
## Absence of proper enquiries and inadequate systems and controls on monitoring and assessing large, unusual or suspicious customer deposits



The LC would:

-  monitor large fund deposits made by its customers into their accounts
-  make enquiries with customers where deposits made by them exceeded the amount of assets declared at their account opening

The SFC's investigation revealed that:



the amounts of deposits made into the accounts of six customers were **incommensurate with their financial profiles** declared in their account opening documents

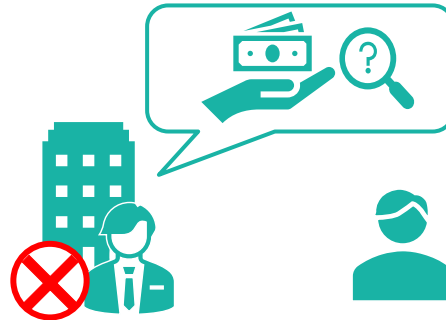
# Case example 1

## Absence of proper enquiries and inadequate systems and controls on monitoring and assessing large, unusual or suspicious customer deposits

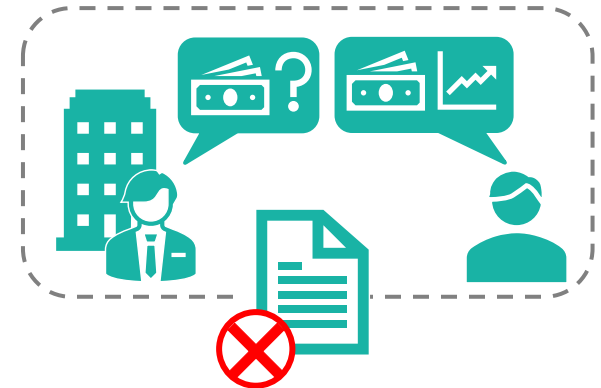
The LC failed to demonstrate that its systems and controls were effective and adequate:



**No written procedures** on monitoring and conducting enquiries on large, unusual or suspicious customer deposits



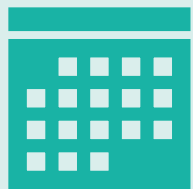
**No internal controls** to ensure its staff followed up with customers to verify their source of funds and documented such enquiries



**No records of enquiries** made by the LC with the customers and **their responses** to the enquiries

# Case example 1

## Ineffective ongoing monitoring system to detect and assess suspicious trading patterns



Between  
**November 2017** and  
**October 2018**



The LC identified over **12,000** self-matched transactions in **10** customer accounts



Self-matched trades refer to those trades where the customer's order matched with his/her own order in the opposite direction



The entry of matching buys and sells orders creates an illusion of trading and is one of the red flags that may give rise to suspicion of money laundering



# Case example 1

## Ineffective ongoing monitoring system to detect and assess suspicious trading patterns

The LC failed to detect those self-matched trades and its systems and controls were inadequate and ineffective:



**No policies and procedures** to guide its staff on the monitoring of customer trading activities to recognise suspicious transactions



**Relied on its responsible officer** to manually review customers' trades who failed to identify the self-matched trades



**Did not activate the function** in its BSS to detect and prevent self-matched trades by its customers

# Case example 1

LCs are reminded to:



# Case example 2



Non-face-to-face  
account opening  
via mobile  
application



Failure to adopt acceptable account opening procedures for verifying the identities of customers who opened their accounts on a non-face-to-face basis through mobile application

# Case example 2

## Deficiencies in account opening procedures

② The LC engaged a Mainland service provider to provide **certification services** for customer identity verification



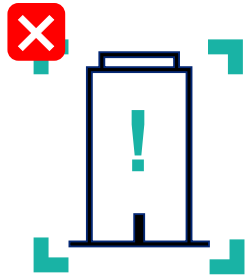
① The LC launched a **mobile application** for **non-face-to-face account opening** for Mainland residents

③ Customers are required to transfer an **initial deposit of not less than HK\$10,000** from a **bank account in their names** to activate the accounts within 30 days

## Case example 2

### Deficiencies in account opening procedures

The identity verification procedures adopted by the LC were deficient, in that:



The certifier engaged by the LC was **not a recognised certification authority**



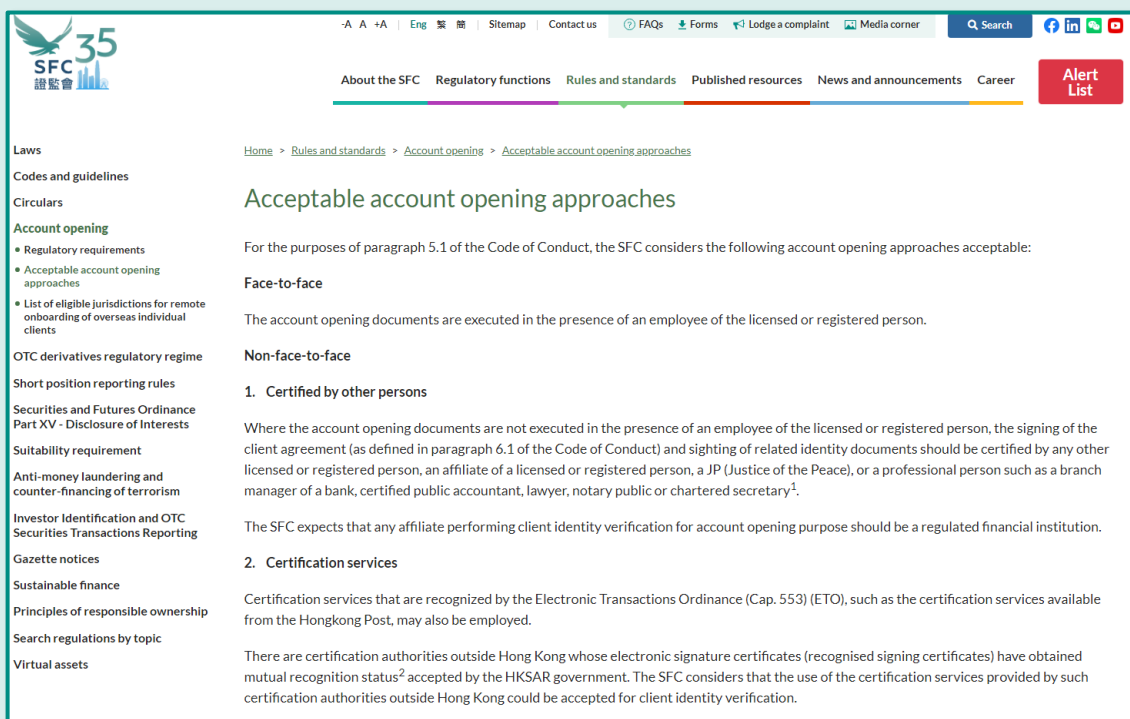
The electronic signature certificates **did not obtain mutual recognition status** accepted by the Hong Kong Government



**37%** of the customers did not transfer an **initial deposit** of not less HK\$10,000 from a bank account in the customer's name maintained with a licensed bank in Hong Kong

# Case example 2

For account opening in a non-face-to-face situation, the SFC sets out a list of approaches that are acceptable, including (among others):



The screenshot shows the SFC website page for 'Acceptable account opening approaches'. The breadcrumb trail is: Home > Rules and standards > Account opening > Acceptable account opening approaches. The page content is as follows:

### Acceptable account opening approaches

For the purposes of paragraph 5.1 of the Code of Conduct, the SFC considers the following account opening approaches acceptable:

#### Face-to-face

The account opening documents are executed in the presence of an employee of the licensed or registered person.

#### Non-face-to-face

- 1. Certified by other persons**

Where the account opening documents are not executed in the presence of an employee of the licensed or registered person, the signing of the client agreement (as defined in paragraph 6.1 of the Code of Conduct) and sighting of related identity documents should be certified by any other licensed or registered person, an affiliate of a licensed or registered person, a JP (Justice of the Peace), or a professional person such as a branch manager of a bank, certified public accountant, lawyer, notary public or chartered secretary<sup>1</sup>.
- 2. Certification services**

Certification services that are recognized by the Electronic Transactions Ordinance (Cap. 553) (ETO), such as the certification services available from the Hongkong Post, may also be employed.

There are certification authorities outside Hong Kong whose electronic signature certificates (recognised signing certificates) have obtained mutual recognition status<sup>2</sup> accepted by the HKSAR government. The SFC considers that the use of the certification services provided by such certification authorities outside Hong Kong could be accepted for client identity verification.



Use certification services provided by certification authorities outside Hong Kong whose electronic signature certificates have obtained **mutual recognition status**



Require customers to transfer an **initial deposit of not less than HK\$10,000** from a bank account in customer's name maintained with a licensed bank in Hong Kong and conduct **all future deposits and withdrawals through this designated bank account only**

A light teal abstract graphic consisting of several overlapping, curved shapes that resemble stylized wings or a bird in flight, positioned on the left side of the slide.

**Thank you.**

**AML/CFT section of the SFC website:**

<https://www.sfc.hk/en/Rules-and-standards/Anti-money-laundering-and-counter-financing-of-terrorism>