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

November 2024

Contents

Glossary of key terms and abbreviations

Terms / abbreviations	Meaning
AI	Artificial intelligence
AML/CFT	Anti-money laundering and counter-financing of terrorism
API	Application programming interface
CDD	Customer due diligence
CRA	Customer risk assessment
HRA	Hong Kong money laundering and terrorist financing risk assessment
LC	Licensed corporation
ML/TF	Money laundering and terrorist financing
NLP	Natural language processing
PEPs	Politically exposed persons
Regulatory technologies or Regtech	Technology-based solutions for compliance with anti-money laundering and counter-financing of terrorism requirements
RPA	Robotic process automation
SFC	Securities and Futures Commission

I. Executive summary

1. Technological developments in the financial sector have been accelerating in recent years, driven by innovation and various needs to increase efficiency, improve customer experience and ensure regulatory compliance.

2. Notably, the adoption of regulatory technologies (hereafter referred to as “Regtech”) has also gained steam, helping financial institutions remain competitive while complying with the evolving regulatory requirements. In this report, unless otherwise specified, the term “Regtech” refers to technology-based solutions for compliance with anti-money laundering and counter-financing of terrorism (AML/CFT) requirements.

3. Since 2020, the Securities and Futures Commission (SFC) has been monitoring the development of Regtech and its adoption by licensed corporations (LCs) to assist them in complying with the AML/CFT requirements. This is accomplished through various initiatives including surveys, engagement with LCs and Regtech solution providers at different junctures.

4. The SFC noted that LCs have made considerable progress in Regtech adoption in recent years, with notable advancements in both the coverage of AML/CFT processes and the types of underlying technologies used in the solutions implemented.

5. From the latest Regtech survey results of 50 selected LCs, most of the surveyed LCs have reported adopting Regtech solutions in at least one of the major AML/CFT processes. Among these processes, name screening has the highest adoption rate (92%), followed by customer due diligence (CDD) (71%), transaction monitoring (69%), management information reporting (43%) and third-party deposit identification and due diligence (34%).

6. Some early adopters of Regtech solutions are making continuous improvements to enhance the functions and optimise their solutions with the use of integrated solutions, application programming interface (API) and more advanced technologies such as artificial intelligence (AI). Many others are starting to explore and adopt simpler Regtech solutions such as robotic process automation (RPA) to meet their AML/CFT compliance needs. The progress we observed demonstrates the industry’s commitment to strengthen its capabilities to combat money laundering and terrorist financing (ML/TF) by adopting Regtech.

7. In general, LCs recognised the benefits of adopting Regtech. Over 85% of the surveyed LCs acknowledged that Regtech has enhanced their ability to identify and manage ML/TF risks, and around 80% indicated that the adoption of Regtech has helped reduce human errors and the resulting unpredictable damages. Over 75% of the surveyed LCs considered Regtech has optimised resource allocation which enables staff to focus on more crucial and high-risk areas. On the other hand, some LCs expressed concerns about their readiness to adopt Regtech. They also indicated that other major barriers included insufficient information on Regtech solutions and how these solutions can assist in the AML/CFT compliance processes.

8. The purpose of this report is to share the SFC's observations of the current state of Regtech adoption in the industry. This includes their key drivers, challenges and considerations throughout the adoption processes. The report also provides illustrative use cases of Regtech solutions that are commonly adopted in major AML/CFT processes by the industry. Our aim is to provide industry practitioners with practical insights to help them adopt Regtech solutions in an effective manner.

9. While recognising the benefits of Regtech adoption, LCs are also reminded to implement Regtech solutions in a responsible manner, considering four key principles. These include ensuring (a) adequate governance and accountability by senior management, (b) ongoing monitoring of Regtech solutions, including AI models, (c) effective data protection and cybersecurity measures for customer and transaction data, and (d) effective management of any risks posed by external vendors.

10. It is important to note that there are no universally applicable Regtech solutions in the market. Given the diverse nature, complexity and scale of LCs' business operations, the decision on whether and how to adopt Regtech should be proportionate, taking into account their unique circumstances. To ensure effective adoption, LCs are encouraged to assess their needs and capabilities, as well as potential costs and benefits of adopting Regtech in the AML/CFT processes.

11. LCs are also reminded that Regtech adoption is not an "all or nothing" approach but can be a gradual process that allows LCs to implement Regtech solutions at their own pace. LCs may focus on specific regulatory and operational challenges and implement Regtech solutions for a particular process, before gradually expanding according to their needs.

12. As one of its strategic priorities, the SFC has also made efforts in adopting technologies to enhance its operational efficiency and strengthen its risk-based supervisory approach. It has automated its workflow and introduced AI to some of its processes, allowing staff to focus on higher-risk areas and more meaningful tasks. For instance, a new platform has been developed to analyse the intelligence from law enforcement agencies and an AI model has been applied to correlate key matters with targeted entities and highlight specific areas that require regulatory attention. All these help the SFC promptly follow up on identified risk attributes.

13. Going forward, the SFC will continue to engage with the industry and stay informed of the latest developments as well as challenges in Regtech adoption. The SFC believes that collaboration with the industry can help uphold the integrity of the financial sector and bolster its capabilities in combatting ML/TF.

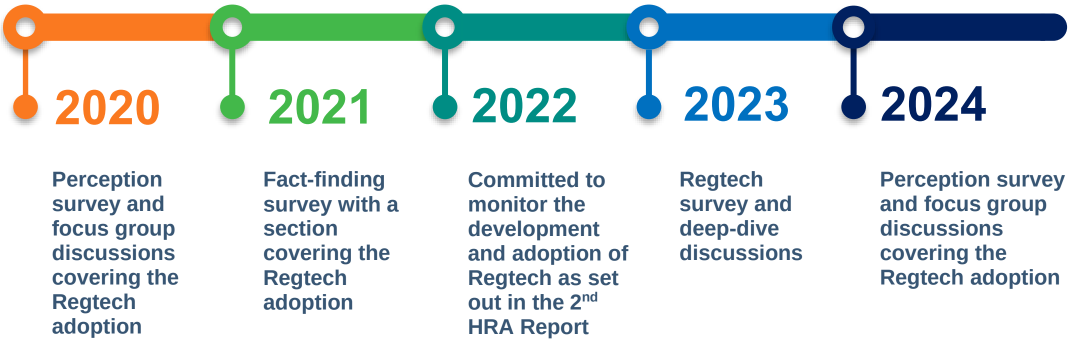
II. Introduction

14. Financial crime is getting increasingly sophisticated. Criminals are utilising more advanced technologies and techniques to commit fraud and launder money. Conventional manual approaches in detecting and preventing money laundering and related predicate offences are becoming less effective.

15. LCs are dealing with an increasing volume of data that encompasses indicators of risk attributes, which often go unnoticed by conventional monitoring methods. Regtech solutions help automate processes and analyse a large volume of data rapidly and consistently, enabling LCs to identify potential ML/TF risks more promptly and accurately.

16. In recent years, the Financial Action Task Force has been actively promoting the awareness of leveraging new and existing technology-based solutions for AML/CFT processes. It encourages the responsible adoption of Regtech to ensure the effective implementation of AML/CFT measures.

17. The SFC has undertaken a number of initiatives to monitor the developments and progress of Regtech adoption, including focus group discussions held in 2020 and 2024, along with the fact-finding, perception and Regtech surveys conducted over the years. These form part of the Hong Kong ML/TF risk assessment (HRA) exercises to understand how Regtech adoption can help mitigate the ML/TF vulnerabilities in the sector.



2020 Perception survey and focus group discussions covering the Regtech adoption

2021 Fact-finding survey with a section covering the Regtech adoption

2022 Committed to monitor the development and adoption of Regtech as set out in the 2nd HRA Report

2023 Regtech survey and deep-dive discussions

2024 Perception survey and focus group discussions covering the Regtech adoption

18. These initiatives have facilitated engagement with industry practitioners and fostered discussions on the benefits and challenges on the Regtech adoption. The SFC would like to thank all the market participants who have contributed to these initiatives.

19. Through these initiatives, the SFC noted that LCs have made considerable progress in Regtech adoption and believes it is now the opportune moment to share its observations on how the industry has embraced the responsible adoption of Regtech over the years, drawing on their success stories with illustrative use cases in major AML/CFT processes.

III. The SFC's observations

A. Background

20. During the second HRA, the SFC obtained an overview of whether and how LCs have adopted Regtech to assist their compliance with the AML/CFT requirements. As set out in the HRA report published in 2022, it was observed that larger-sized LCs, particularly brokerages with larger client bases and a high volume of transactions, had a higher level of Regtech adoption.

21. From its ongoing engagement with the industry in recent years, the SFC observed that LCs have made considerable progress in Regtech adoption. In particular, there are notable advancements in both the coverage of AML/CFT processes and the types of underlying technologies used in the solutions implemented.

22. In mid-2023, the SFC conducted a more comprehensive Regtech survey on 50 selected LCs (surveyed LCs). They were selected based on several criteria, including the types of regulated activities that they engage in, company background[1], business and operation sizes, clientele and their Regtech adoption experience gathered in the previous engagements.

23. The survey aimed to gauge the LCs' adoption status of Regtech in the AML/CFT processes[2] 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.

24. With reference to the survey results, surveyed LCs were selected for deep-dive discussions to obtain a more comprehensive understanding of their adoption approach. This included how the implemented Regtech solutions have assisted them in major AML/CFT processes, their key considerations for implementation, and how they have overcome the challenges encountered.

25. The sections below summarise the key observations on the benefits and challenges of Regtech adoption and the common types of Regtech solutions gathered from the Regtech survey, deep-dive discussions and other engagement sessions with LCs.

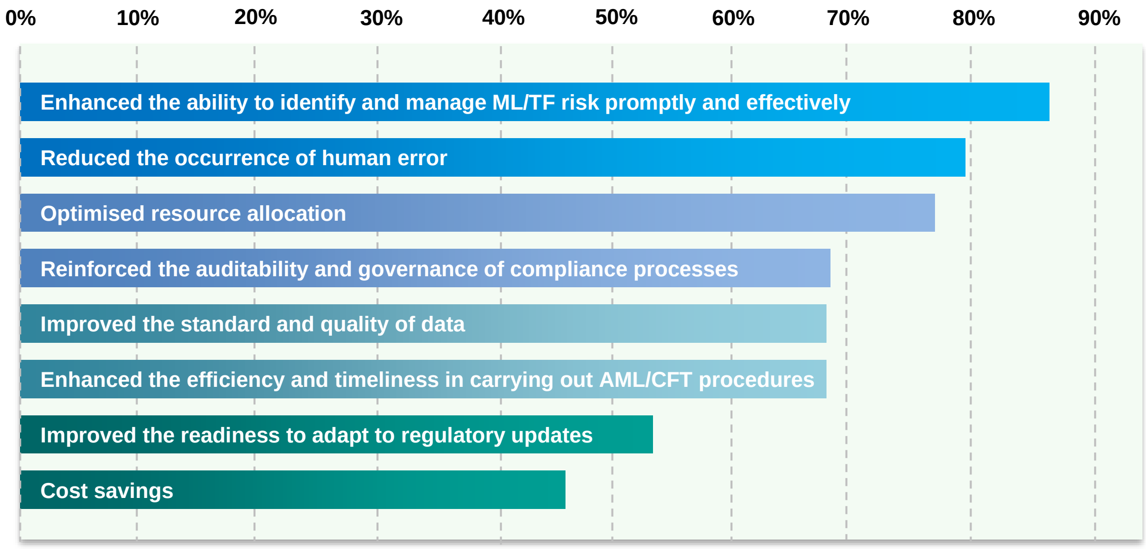
[1] For example, some LCs are standalone companies while others are part of a multi-national financial group or Mainland-based financial group.

[2] For the purpose of this survey, we primarily focused on the following five major AML/CFT processes:
- CDD;
- name screening;
- transaction monitoring;
- third-party deposits identification and due diligence; and
- management information reporting.

B. Benefits and challenges of Regtech adoption

26. As indicated in the survey results below, the majority of the surveyed LCs agreed that Regtech adoption has resulted in a broad range of operational benefits.

Benefits of Regtech adoption



27. Specifically, over 85% of the surveyed LCs considered that Regtech solutions have enhanced their ability to identify and manage ML/TF risks promptly and effectively. Around 80% of them indicated that the automation of certain AML/CFT procedures has reduced the occurrence of human errors and the resulting unpredictable damages. More than 75% of them also considered that Regtech adoption could optimise resource allocation, enabling staff to focus on more crucial and higher ML/TF risk areas.

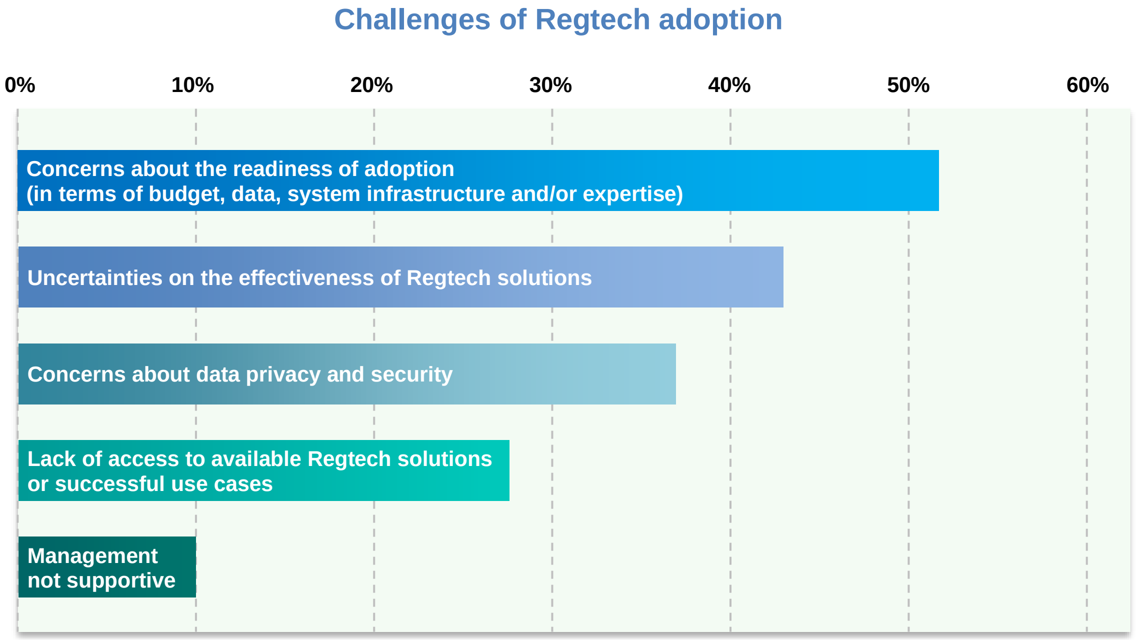
28. Furthermore, nearly 70% of the surveyed LCs believed that Regtech adoption has reinforced the auditability and governance of their compliance processes. It has also improved the standard and quality of data maintained within the firms. This is primarily attributed to the digitisation and standardisation of customer and transaction data required at the initial stages of Regtech adoption.

29. Nearly 70% of the surveyed LCs agreed that Regtech solutions have enhanced the operational efficiency and timeliness in carrying out the AML/CFT procedures, and largely reduced the number of overdue review cases. Some LCs specifically mentioned that this has benefited the process owners across compliance, business, operations and finance departments. In addition, customer experience has improved due to streamlined onboarding processes, and the number of false positive alerts arising from name screening process have reduced.

30. More than half of the surveyed LCs also indicated that Regtech solutions have improved their readiness to adapt to regulatory updates. This was because some solution providers would provide timely updates on regulatory changes and introduce modified or new modules to integrate with their existing solutions.

31. Less than half of the surveyed LCs considered that Regtech adoption could result in cost savings, and some indicated the initial implementation cost may not be low. However, most of them believed that adopting Regtech solutions is a long-term investment which can ultimately help save costs, especially in terms of time and resources.

32. Despite numerous benefits that encourage Regtech adoption, there are challenges which are shown in the survey results below.



33. Approximately half of the surveyed LCs expressed concerns about their readiness of adoption in terms of budget, data, system infrastructure and/or expertise. Some LCs specifically mentioned that having the right mentality is the key to getting themselves ready in all aspects. To address this challenge, they engaged with all stakeholders (eg, business, compliance, operations and finance departments) to identify the needs of adopting Regtech such as streamlining and automating workflows, and deduce the long-term benefits. They also shared that the Government has provided funding programmes to support the use of technological solutions.

34. In addition, these LCs met with in-house IT and/or external vendors to explore how they could improve their readiness by digitising and standardising relevant data as well as upgrading their system infrastructure. They also consulted these IT experts on the types of Regtech solutions that could help achieve their objectives and the adoption approach such as whether to develop the solution in-house, subscribe to a readily available solution (including cloud-based solution and on-premises software) or develop a customised solution with an external vendor.

35. Some LCs also chose to start modestly by implementing Regtech solutions in one or a few AML/CFT processes initially. This approach can reduce initial costs and make it easier to showcase progress and demonstrate successful use cases of effective adoption. They also monitored the implemented solutions regularly to ensure they function as intended and refined the algorithms and logics when needed to ensure they are effective. All these also address concerns about the uncertainties on the effectiveness of Regtech solutions in assisting them to fulfil their regulatory obligations, which is one of the challenges raised by 40% of the surveyed LCs.

36. About 35% of the surveyed LCs raised concerns about data privacy and security, especially for cloud-based solutions provided by external vendors. Some LCs addressed these concerns by considering vendors with a proven track record of data privacy and security. For instance, conducting due diligence on the vendors, reviewing their security policies and procedures and understanding their approach to data privacy and security. Some LCs also raised questions on the location of the servers for data storage to ascertain if the servers are located in jurisdictions with weaker data privacy laws or regulations.

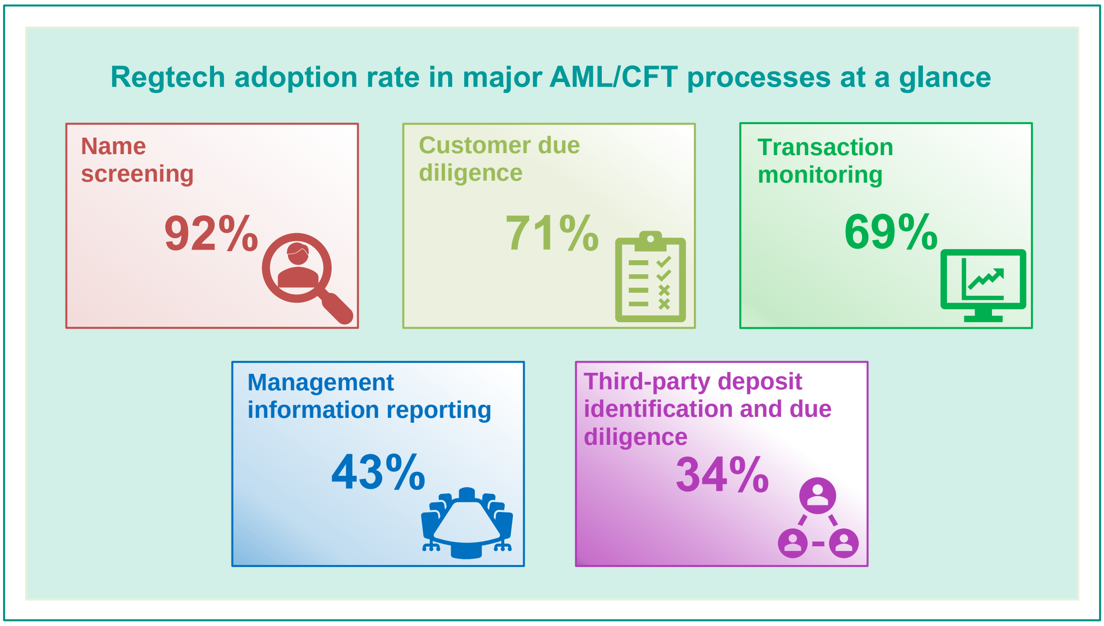
37. While over 25% of the surveyed LCs felt that they lacked access to available Regtech solutions and successful use cases, some said that they would learn from other industry practitioners who have successfully adopted Regtech solutions through networking, attending industry conferences and events, and engaging with Regtech service providers.

38. It is worth noting that most surveyed LCs did not consider lack of management support to be a major barrier. This indicates that management acknowledges the importance and benefits of adopting Regtech. Some LCs also emphasised that the "tone from the top" is crucial in initiating the adoption process. They particularly highlighted the importance of conveying the message that automation and enhancing operational efficiency with Regtech adoption do not equate to reducing manpower or replacing human efforts.

39. The SFC believes that sharing success stories from early adopters and providing illustrative use cases would help address these challenges. The information and insights provided in the following sections serve as a good reference for LCs that are considering adopting or enhancing their Regtech solutions in the AML/CFT processes.

C. Common types of Regtech solutions adopted in major AML/CFT processes

40. As briefly mentioned in the introduction section of this chapter, the SFC has observed considerable progress in Regtech adoption. Most of the surveyed LCs have reported adopting Regtech solutions in at least one of the major AML/CFT processes. Name screening has the highest adoption rate among the AML/CFT processes, followed by CDD and transaction monitoring.



Regtech adoption rate in major AML/CFT processes at a glance

Name screening 92%

Customer due diligence 71%

Transaction monitoring 69%

Management information reporting 43%

Third-party deposit identification and due diligence 34%

i. Name screening

41. Name screening is a key AML/CFT process to identify customers and their beneficial owners or connected parties who are terrorist suspects, possible designated parties, politically exposed persons (PEPs) or associated with adverse media exposure. Most of the surveyed LCs (92%) have indicated that they have adopted Regtech solutions in name screening.

Key observations on name screening

Name screening

Adoption rate

92% (45 respondents)

36

out of 45 respondents (80%) have adopted Regtech solutions in this area for five years or more

Top three common functions:

- identifying names with alterations
- 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

30

out of 45 respondents (67%) took less than a year from decision to implementation of Regtech solutions

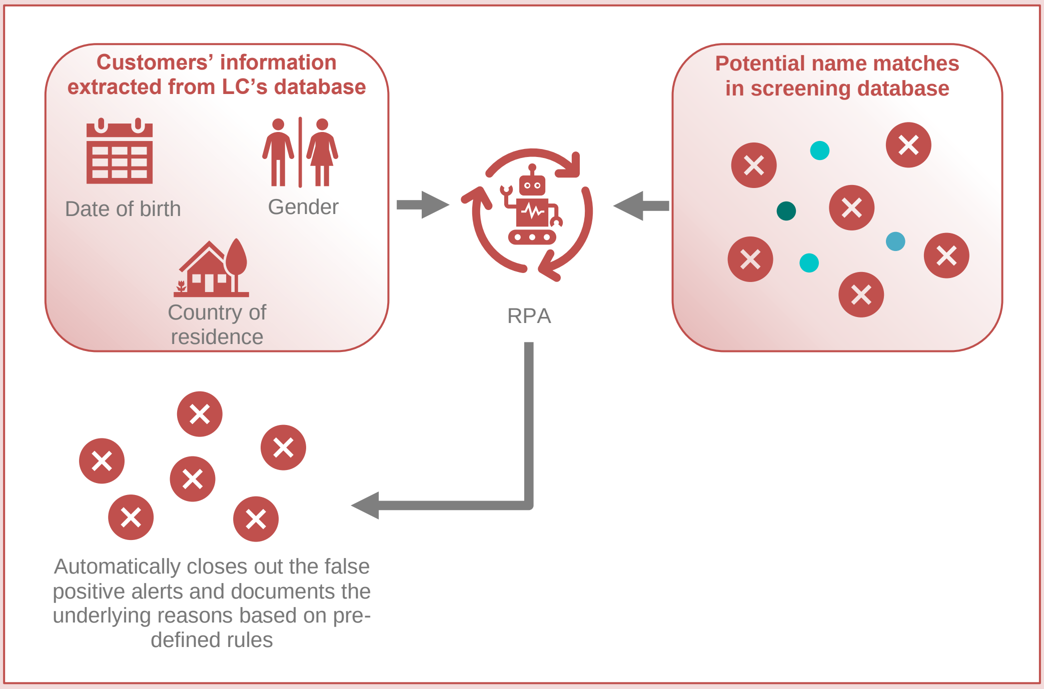
42. Compared to the other AML/CFT processes, Regtech solutions for name screening are more mature because a high number of false positive alerts is a common pain point for LCs. The process is relatively straight-forward and relies on relatively standard data points, such as names and dates of birth of customers, which are often readily available and can be easily processed into Regtech solutions.

43. In general, LCs considered that Regtech solutions can improve the accuracy of name screening by implementing risk-based fuzzy logic to identify potential matches even when the names are misspelt or have minor alterations. These solutions can also capture new and updated designations and automate the ongoing screening on a more timely basis. Some LCs adopted advanced functions to reduce false positive alerts and prioritise the screening alerts based on risk scores, such as applying machine learning to evaluate the likelihood of an alert to be false positive by considering the customer profile.

44. While the scale, complexity and extent of Regtech adoption for the name screening process vary among LCs, they generally recognised that these solutions can significantly enhance efficiency and effectiveness by reallocating resources to review screening alerts with higher risks or more likely to be true hits.

Illustrative use cases of Regtech solutions adopted by LCs for name screening

Example 1: Implementing RPA which automatically closes out alerts with mismatched information

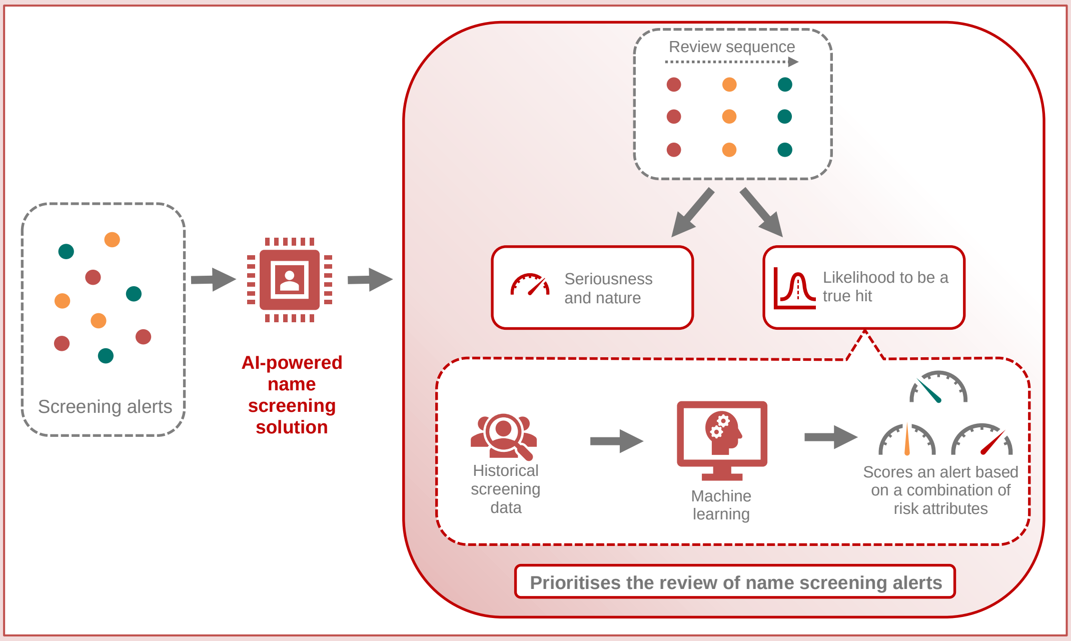

Customers' information extracted from LC's database
Date of birth
Gender
Country of residence
RPA
Potential name matches in screening database
Automatically closes out the false positive alerts and documents the underlying reasons based on pre-defined rules

An LC has implemented RPA in the name screening process to extract relevant customer information and compare to the alert profile. In addition to names, the LC's RPA bot is programmed to take into account an individual's identification information such as the date of birth or age, gender and country of residence.

Any alerts with obvious mismatches in other identification information would be treated as false positive alerts. The RPA bot will automatically close out these false positive alerts and document the underlying reasons based on pre-defined rules. For instance, if the age in the alert profile exceeds the predetermined tolerance level for age difference, the RPA bot will record the predefined reasoning, such as "The customer does not match the individual identified in the potential match due to the age difference.", and close out the alert.

The LC considered that the implementation of RPA in name screening is relatively simple and affordable. It has largely enhanced the accuracy of the name screening process and expedited the process by significantly reducing the time spent in reviewing false positive alerts, as well as ensuring consistent decisions in closing out the alerts.

Example 2: AI-powered name screening solution

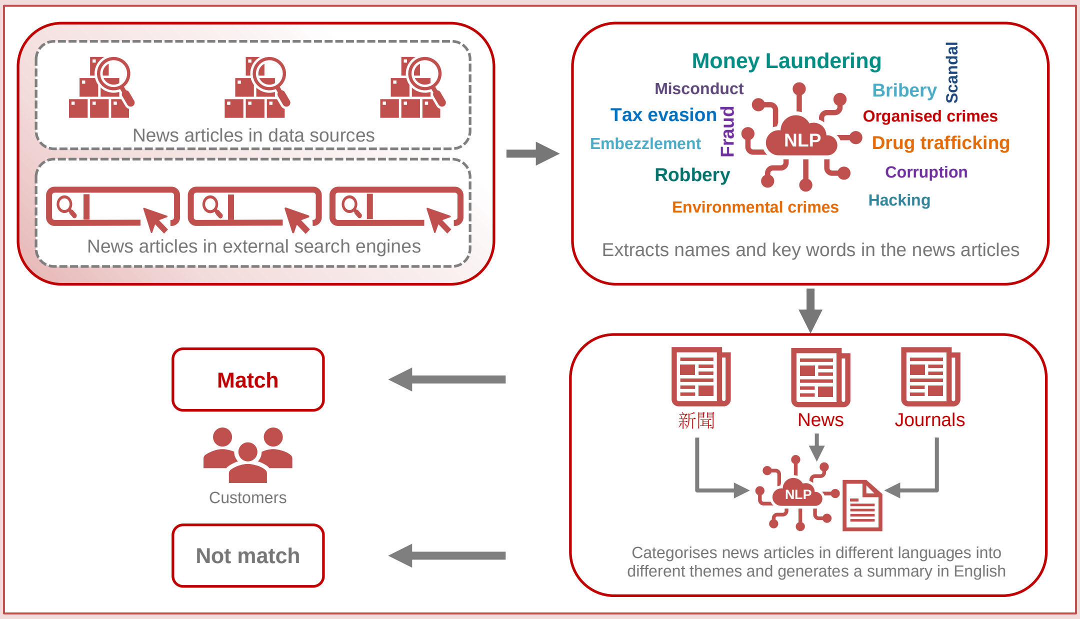

Screening alerts
AI-powered name screening solution
Review sequence
Seriousness and nature
Likelihood to be a true hit
Historical screening data
Machine learning
Scores an alert based on a combination of risk attributes
Prioritises the review of name screening alerts

An LC has implemented an AI-powered name screening solution to distinguish true hits from system-generated alerts. This solution helps prioritise the review of name screening alerts based on the nature of the alerts (ie, sanctions, PEPs or adverse media-related) and the likelihood of a true hit with reference to historical data.

By training machine learning models based on historical screening data, the solution can determine the likelihood of a true hit with a higher accuracy. The alerts would be scored based on a combination of risk attributes for prioritising the review of highly probable true hits.

The LC considered that the AI-powered solution has largely improved the efficiency of name screening process and prioritised efforts for possible true hits. It also identifies potential high-risk cases more accurately by capturing scenarios with minor variations or alterations in certain data points.

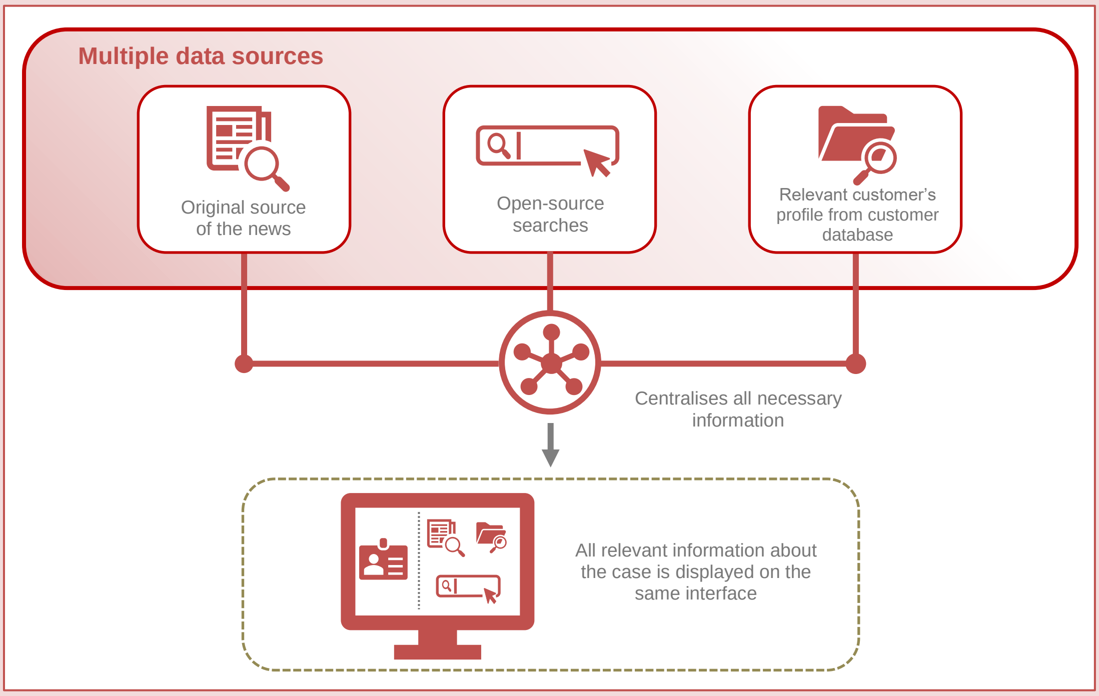
Example 3: Natural language processing (NLP) engine in adverse media screening solution


News articles in data sources
News articles in external search engines
Money Laundering
Misconduct
Bribery
Scandal
Tax evasion
Fraud
Organised crimes
Embezzlement
NLP
Drug trafficking
Robbery
Corruption
Environmental crimes
Hacking
Extracts names and key words in the news articles
Match
Customers
Not match
新聞
News
Journals
NLP
Categorises news articles in different languages into different themes and generates a summary in English

An LC has deployed a news screening solution provided by an external vendor. This solution supports more than 40 languages and connects multiple external search engines and data sources. To identify adverse news relating to the LC's customers, the solution utilises an NLP engine to extract names and key words in news articles. The engine can also categorise news articles in different languages and generate a concise summary in English, covering global news while streamlining the case review process. Moreover, it can identify duplicated news to prevent redundant review of similar articles.

The LC considered that the NLP engine has improved the efficiency of processing a significant volume of news articles while identifying relevant adverse news more accurately. It also provides flexibility to optimise screening results through editing the keyword library or adjusting match strength.

Example 4: Customised workflow tool to streamline the adverse media review process


Multiple data sources
Original source of the news
Open-source searches
Relevant customer's profile from customer database
Centralises all necessary information
All relevant information about the case is displayed on the same interface

An LC has engaged an external vendor to develop a customised workflow tool which streamlines the adverse media review process. The workflow tool centralises all necessary information in a single platform which eliminates the need to check multiple information sources during case review, such as referring to the original news source, performing open-source searches, and accessing the customer database for the customer's profile. All relevant information about the case is now displayed on the same interface, allowing users to efficiently compare the information side-by-side.

The platform also supports the extraction of available images from news articles or open-source information. This enables direct comparison with the customer's image per the identification document stored in the LC's database.

In the customised workflow tool, there is also a dropdown menu with a list of pre-defined rationales for users' selection when closing out the alerts.

ii. CDD

45. According to our survey results, over 70% of the surveyed LCs indicated that they have implemented Regtech solutions in their CDD process, including the onboarding of individual customers, customer risk assessment (CRA) and ongoing monitoring measures.

46. LCs commonly start adopting Regtech solutions at the onboarding stage as part of their digitisation process. Customer data collected during onboarding facilitate the AML/CFT processes at the subsequent stages. The use of Regtech solutions expedites the customer onboarding process by automating the data collection process, and provides a more comprehensive view of customer risk profiles. This enables LCs to identify and manage potential risks more effectively and holistically. It also helps maintain a clear audit trail to demonstrate compliance with the relevant CDD requirements.

Key observations on CDD

Customer due diligence

Adoption rate

71% (35 respondents)

24

out of 35 respondents (69%) took less than a year from decision to implementation of the Regtech solutions

25

out of 35 respondents (71%) indicated that their solutions can facilitate onboarding of individual customers

29

out of 35 respondents (83%) indicated that their solutions can facilitate customer risk assessment

30

out of 35 respondents (86%) indicated that their solution can facilitate CDD and ongoing monitoring measures

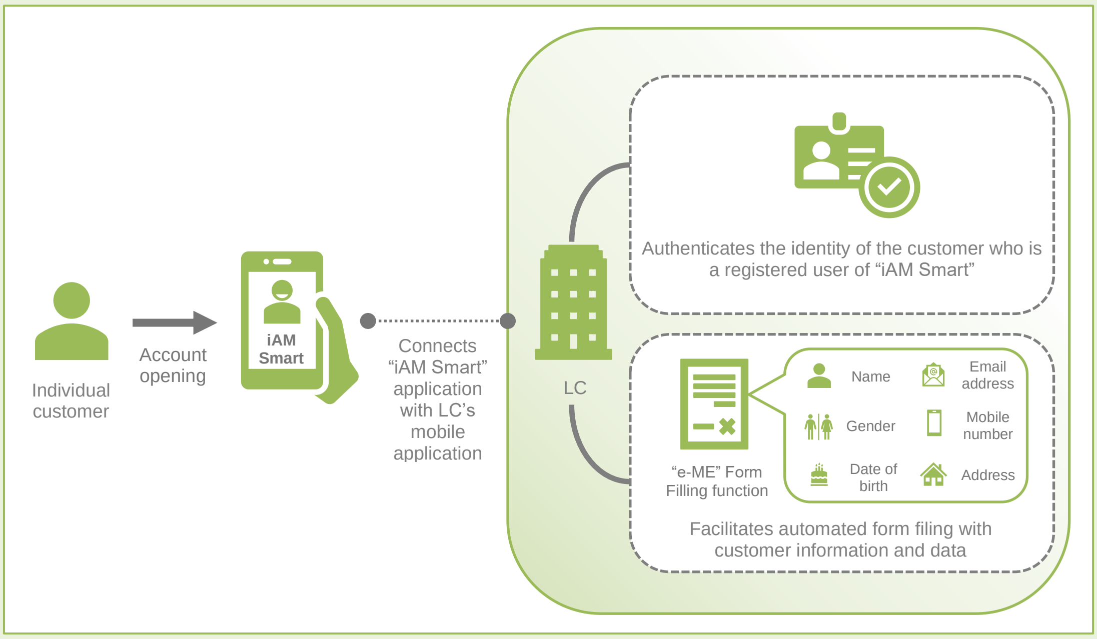
47. Some surveyed LCs indicated that their Regtech solutions have assisted in verifying or authenticating a customer’s identity using, for instance, iAM Smart or biometric recognition. Some solutions also enabled automated background checks by utilising public sources, such as litigation records and cold shoulder orders, and comparing the results of the background checks with the customer’s information. In addition, some LCs employed analytics solutions to facilitate ongoing CDD reviews or detect situations which warrant trigger event-driven reviews. Case management tools are another example of Regtech solution for documenting and tracking onboarding and ongoing monitoring processes.

48. CRA typically occurs after LCs gather customer data during the onboarding process. Some LCs adopted Regtech solutions for CRA which help analyse customer data more comprehensively and accurately. Risk re-rating would also be automatically triggered when there are changes of customer information to ensure that a customer's ML/TF risk profile is promptly updated. This enables more timely and effective identification of potential ML/TF risks while reducing the risk of overlooking any embedded risk attributes in a customer's profile.

49. LCs considered that Regtech solutions also help ensure consistent application of the risk assessment methodology across different customers and different time periods, avoiding biases and risks of manual calculation errors.

Illustrative use cases of Regtech solutions adopted by LCs for client onboarding and CRA

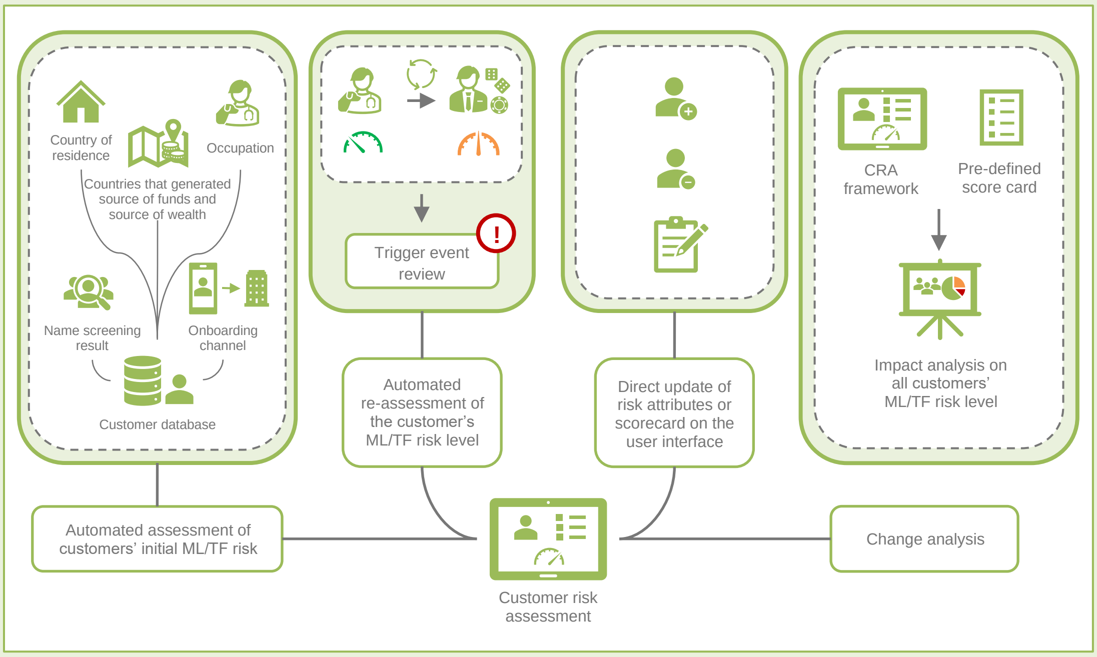
Example 5: Identity verification and automated form filling through adoption of "iAM Smart"


Individual customer
Account opening
iAM Smart
Connects "iAM Smart" application with LC's mobile application
LC
Authenticates the identity of the customer who is a registered user of "iAM Smart"
"e-ME" Form Filling function
Name
Email address
Gender
Mobile number
Date of birth
Address
Facilitates automated form filing with customer information and data

"iAM Smart" is an SFC's recognised digital identification system since June 2023. An LC has established API connection between its mobile application and the "iAM Smart" application to authenticate the identity of a customer who is a registered user of "iAM Smart". The "e-ME" Form Filling function also facilitates automated form filling with customer information and data (such as English name, Chinese name, gender, identity card number, date of birth, email address, mobile phone number, residential address), which expedites the account opening process and ascertains the accuracy and reliability of customer information.

As the registered users of "iAM Smart" exceeded three million as of August 2024, the LC believed this is a simple and economical way to enable remote customer onboarding without requiring its customers to make an initial deposit of not less than HK$10,000 from the customer's designated bank accounts in Hong Kong.

Example 6: Automated customer risk assessment


Country of residence
Occupation
Countries that generated source of funds and source of wealth
Name screening result
Onboarding channel
Customer database
Trigger event review
Automated re-assessment of the customer's ML/TF risk level
Direct update of risk attributes or scorecard on the user interface
CRA framework
Pre-defined score card
Impact analysis on all customers' ML/TF risk level
Automated assessment of customers' initial ML/TF risk
Customer risk assessment
Change analysis

An LC has implemented an automated CRA process which also enables dynamic tracking of customers' ML/TF risk profile.

Risk score is assigned to each of the identified risk attributes using a pre-defined scorecard. Customers' initial ML/TF risk can be assessed automatically based on risk attributes relating to pertinent data extracted from the customer database. Such risk attributes include country of residence, countries from which the customer generates source of funds and source of wealth, occupation, name screening results as well as onboarding channel.

Furthermore, the customer's ML/TF risk level would be automatically re-assessed when changes in the risk attributes of the customer data are detected (eg, updates in occupation, changes in the jurisdiction that generate the customer's source of funds). Notification would be sent to trigger enhanced due diligence measures when the customer's ML/TF risk level is elevated.

The solution also enables adding or removing of risk attributes, or adjusting the scorecard directly on the user interface, subject to appropriate approval. It also supports the LC to conduct change analysis to evaluate the overall impact on all customers' ML/TF risk level upon updates on the CRA framework and pre-defined scorecard.

iii. Transaction monitoring

50. Transaction monitoring is an important AML/CFT process to detect unusual or suspicious transactions and activities which may indicate ML/TF. Based on our survey results, nearly 70% of the surveyed LCs have adopted Regtech solutions to enhance the accuracy and efficiency of their transaction monitoring process while the extent and complexity of the solutions may differ.

Key observations on transaction monitoring

Transaction monitoring

Adoption rate

69% (34 respondents)

22

out of 34 respondents (65%) 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 transaction monitoring alerts to be reviewed and/or investigated according to the handling priority

51. In terms of functions, most surveyed LCs adopted Regtech solutions to generate alerts of potential unusual or suspicious transactions based on pre-defined rules and scenarios. Some LCs improved the process by using case management tools to document and track the handling of alerts, while others used more advanced functions to triage the alerts for review based on risk scores.

52. Traditionally, LCs have commonly used rule-based transaction monitoring solutions that rely on a single parameter, such as large transaction amounts, frequent deposits or withdrawals, transactions involving high-risk jurisdictions, to flag transactions which meet specific thresholds.

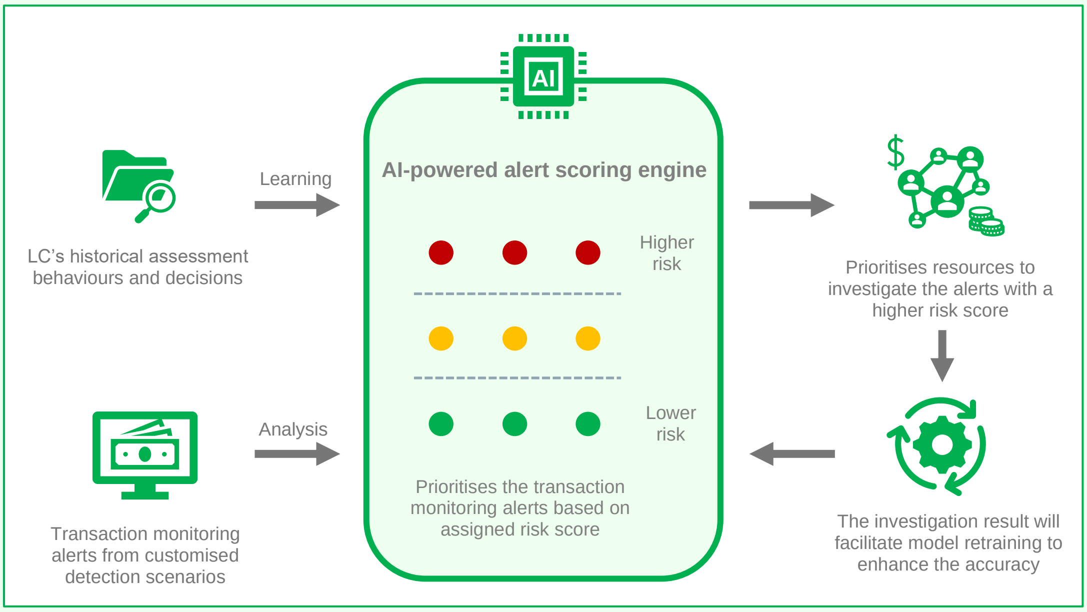
53. However, some LCs recognised the limitations of traditional rule-based transaction monitoring solutions which generated a significant number of false positive alerts. For example, the rule setting did not support the scenarios with dynamic parameters taking into account a customer’s profile or usual transaction patterns. Also, rule-based solutions may not be effective in adapting to changing ML/TF risks or new types of transaction behaviour, making them less capable of identifying emerging risks or sophisticated ML/TF schemes and related predicate offences.

54. To address these challenges, some LCs have started adopting Regtech solutions with more advanced underlying technologies, eg, AI, in their transaction monitoring process. For instance, machine learning algorithms are used to analyse large volumes of transaction data and identify behavioural patterns that may indicate potential ML/TF risks. These algorithms can be trained to learn from historical transactions and identify suspicious patterns or behaviour as they emerge, enabling more effective detection of anomalies in a timely manner.

55. Some LCs have also adopted other AI features to enhance their transaction monitoring processes, for example, to prioritise alerts based on their risk score and filter out false positive alerts, allowing staff to focus on transactions of higher risks.

Illustrative use cases of Regtech solutions adopted by LCs for transaction monitoring

Example 7: Transaction monitoring solution with an AI-powered alert scoring engine


AI
AI-powered alert scoring engine
LC's historical assessment behaviours and decisions
Learning
Higher risk
Lower risk
Transaction monitoring alerts from customised detection scenarios
Analysis
Prioritises the transaction monitoring alerts based on assigned risk score
Prioritises resources to investigate the alerts with a higher risk score
The investigation result will facilitate model retraining to enhance the accuracy

An LC has implemented a transaction monitoring solution which generates alerts based on a set of customised detection scenarios with dynamic parameters, for example, to identify unusual large deposits by comparing with the average of the customer's aggregated transaction amount in the past three months.

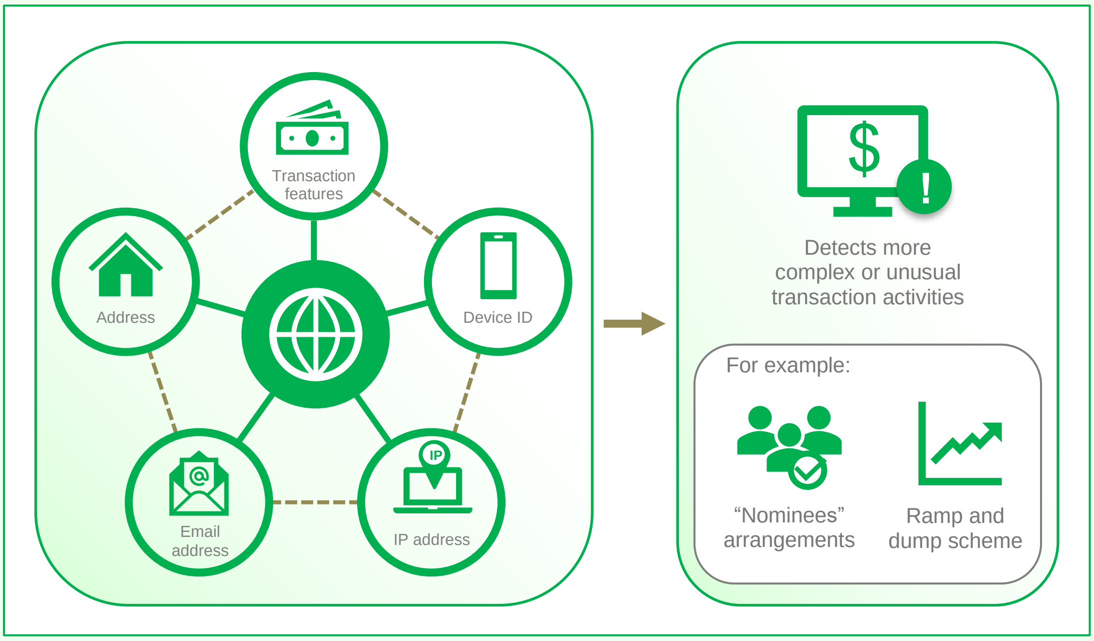
The solution utilises an AI-powered alert scoring engine. The underlying machine learning model is trained to identify red flags in transactions and learns from the LC's historical assessment behaviours and decisions, to determine a risk score. The LC will prioritise resources to review the alerts with a higher risk score. The alert review results will form part of the data to retrain the machine learning model to enhance its accuracy in identifying red flags and alert scoring.

For alerts with a lower risk score, the rule engine in the transaction monitoring solution could automatically discount the alerts if the concerned transactions are in line with the customer's profile or typical transaction behaviours (eg, large transactions for a specific stock that the customer has previously traded).

Furthermore, the solution facilitates the identification of unusual or suspicious transaction patterns across multiple accounts belonging to or related to the same customer, enabling a holistic monitoring at customer level.

The LC considered that the transaction monitoring solution with an AI-powered alert scoring engine has enhanced the overall effectiveness and efficiency of the process, enabling staff to focus on transactions that genuinely carry higher risks.

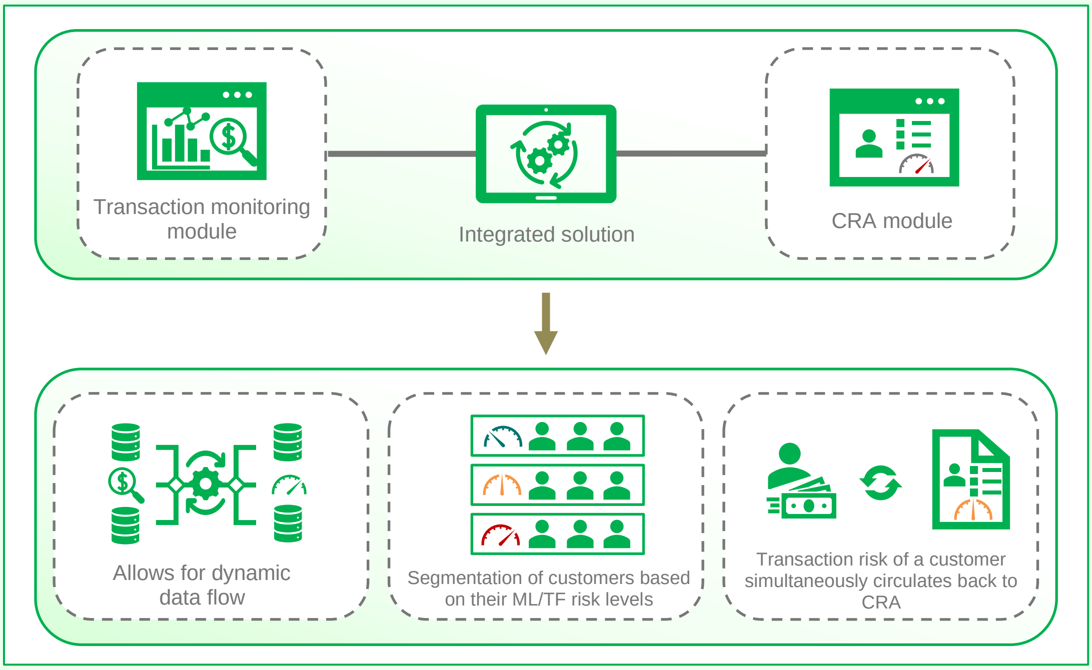
Example 8: Use of network analytics for transaction monitoring



An LC has utilised network analytics in the transaction monitoring process. Network analytics can help identify hidden relationships between customers by connecting commonalities of customer information such as same address, contact number, email address, IP address or device ID, and transaction characteristics such as same stock, similar quantity or transaction time. Upon receiving requests from law enforcement agencies or SFC for information regarding a customer's transactions on a specific stock, the LC would utilise the analytics solution to identify customers who may appear unrelated for enhanced monitoring or further investigations.

The LC considered network analytics effective in detecting more complex or unusual transaction activities such as "nominees" arrangements, ramp and dump schemes, which cannot be easily identified through traditional rule-based solutions.

Example 9: Integrated solution for CRA and transaction monitoring system


Transaction monitoring module
Integrated solution
CRA module
Allows for dynamic data flow
Segmentation of customers based on their ML/TF risk levels
Transaction risk of a customer simultaneously circulates back to CRA

An LC has implemented an integrated solution that connects the CRA module with transaction monitoring module. This integration allows for dynamic data flow, enabling the segmentation of customers based on their ML/TF risk levels. By applying different thresholds to customers based on segmentation results, the LC considered it more effective in monitoring their transactions in a risk-based manner.

In addition, the transaction risk associated with a customer can be simultaneously circulated back into the CRA. This would trigger enhanced measures if the risk level is elevated. For example, the customer risk would be elevated automatically when a suspicious transaction report has been filed on the customer's previous transactions.

The LC recognised that this integration provides a more holistic view of a customer's ML/TF risk profile and facilitates risk-based monitoring of customer activities, minimising the chances of overlooking any emerging risk indicators.

iv. Management information reporting

56. Senior management plays a crucial role in overseeing and ensuring an LC's compliance with the AML/CFT requirements. It is important to keep senior management informed and updated on business developments and regulatory compliance situations. According to our survey results, less than half of the surveyed LCs have adopted Regtech solutions in this area.

Key observations on management information reporting

Management information reporting

Adoption rate

43% (21 respondents)

15

out of 21 respondents (71%) indicated that their solutions can facilitate ML/TF risk metrics generation for reporting purposes

20

out of 21 respondents (95%) indicated that their solutions are either developed by in-house development team or jointly developed with external development team

15

out of 21 respondents (71%) took less than a year from decision to implementation of the Regtech solutions

57. The lower adoption rate of Regtech solutions for management information reporting may be attributed to the involvement of a large amount of data which requires integrated solutions and collaboration with various stakeholders within an LC.

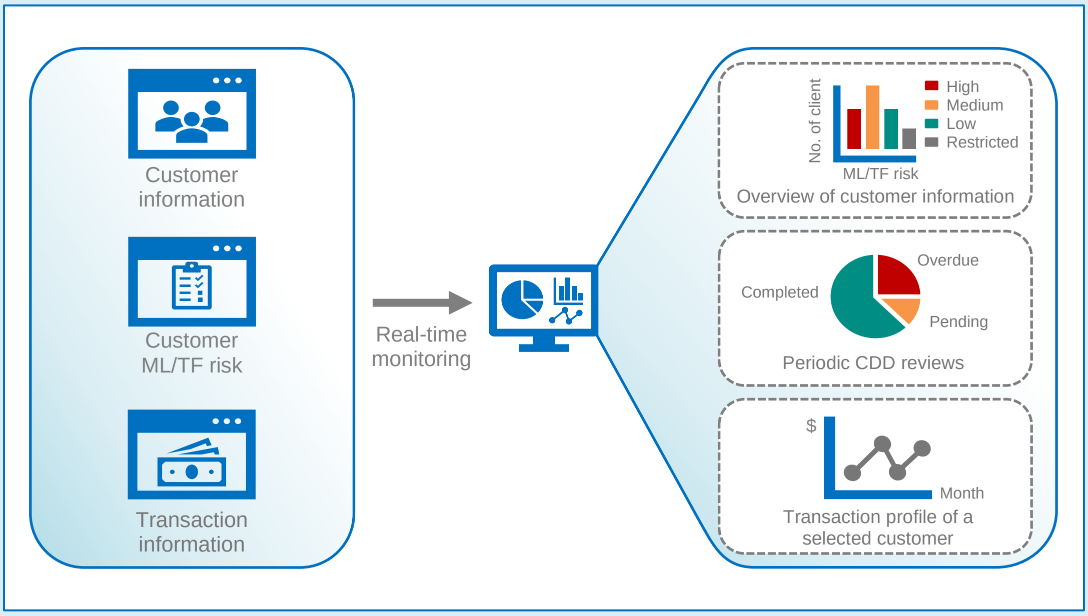
58. LCs are more used to preparing management information reports manually by summarising the key updates for senior management, which can be quite time consuming and prone to errors. These reports include key statistics such as newly onboarded customers, pending review cases for name screening and transaction monitoring alerts, suspicious transaction reports filed, and overdue cases.

59. Some LCs recognise the benefits of adopting Regtech solutions, such as data analytics dashboards. This facilitates the analysis, understanding, and managing of AML/CFT compliance risks of an LC holistically. It also saves time by eliminating the preparation of multiple management information reports which can be duplicative.

60. These LCs also utilise the data and information from the data analytics dashboards to facilitate their performance of institutional risk assessment, compilation of statutory returns such as the Business and Risk Management Questionnaire and performance of other data analytics for business development purpose. These data and information also provide insight into areas for improvement, which helps strengthen LCs' compliance capabilities and enables a more effective implementation of LCs' risk-based approach.

Illustrative use case of Regtech solutions adopted by LCs for management information reporting

Example 10: Management information system using a dynamic dashboard with real-time data feed



An LC has gone through a digitisation process including data standardisation across different systems. All data attributes are collated into an interactive dashboard for real-time monitoring of status and metrics of different processes including CDD, CRA and transaction monitoring.

The dashboard also offers easy navigation and drill-down capabilities. It provides an overview of customers' information such as the number of customers categorised by ML/TF risk levels, customer types and demographics, and sets out periodic CDD reviews that are pending for handling or overdue.

The dashboard also shows the comprehensive profile of a selected customer including transaction history and potential relationships with other customers, such as those trading the same stocks at a similar time or using the same device for trading. This enables more in-depth analysis of specific data points or trends, enhancing the understanding of potential risks and areas for improvement.

By providing a comprehensive view, the dashboard allows senior management to effectively monitor and track the progress of various AML/CFT processes. For instance, this helps identify if there is a relatively higher number of overdue periodic CDD review cases for a particular line of business. It also supports the generation of customised reports to meet the specific needs of different stakeholders, ultimately enabling senior management to make informed decisions leveraging the insights derived from the data.

v. Third-party deposit identification and due diligence

61. Third-party deposits for investment transactions may be used to disguise the true beneficial owner or the source of illicit funds. According to the survey results, a lower percentage of surveyed LCs (34%) have reported the adoption of Regtech solutions for the purpose of identifying the source of deposits or conducting the necessary due diligence process.

Key observations on third-party deposit identification and due diligence

Third-party deposit identification and due diligence

Adoption rate^

34% (14 respondents)

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

12

out of 14 respondents (86%) indicated that their solutions are either developed by in-house development team or jointly developed with external development team

10

out of 14 respondents (71%) took less than one year from decision to implementation of the Regtech solutions

62. Regtech adoption in this area is relatively less mature than other AML/CFT processes, 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. Nevertheless, it is worth noting that around 71% of those adopting Regtech in this area were able to implement the solution within a year. This suggests that the technical aspects involved may not be overly complicated.

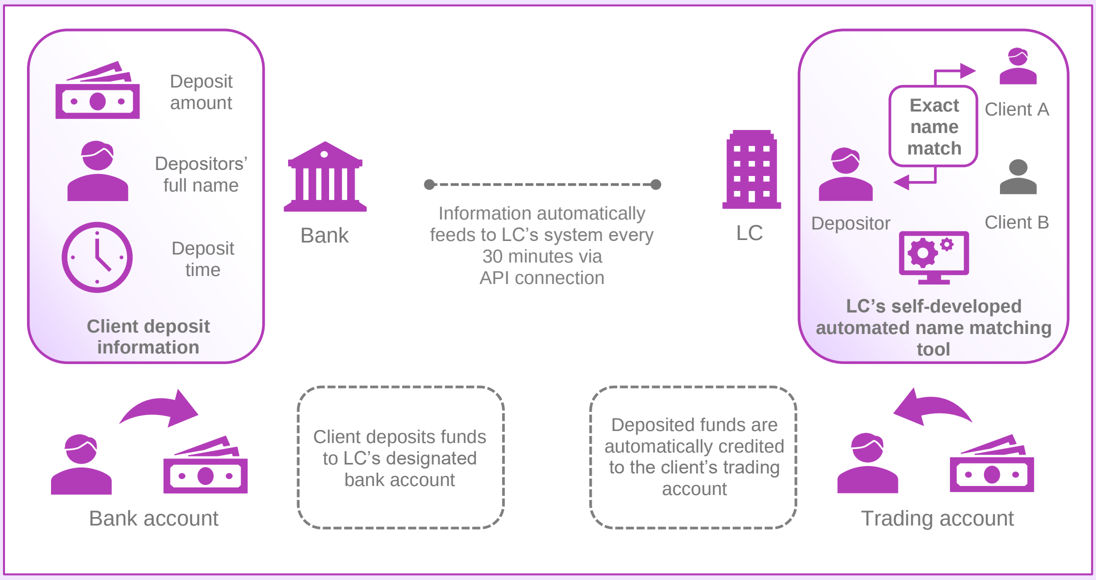
63. LCs have commonly required their customers to submit supporting documents, such as copies of deposit slips or cheques, or screenshots of e-banking transfer records. These documents help LCs identify the sources of deposits and determine whether the funds are from the customer or third parties. However, this manual process is not time sensitive, which creates challenges for LCs trying to promptly identify the source of deposits before settling transactions with the deposited funds.

64. To streamline the process, some LCs, particularly for larger brokerages handling a large number of customer deposits daily, have chosen to implement Regtech solutions to automate the verification of deposit sources.

65. Other LCs have also 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. This provides a structured framework and helps safeguard against potential non-compliance risks.

Illustrative use cases of Regtech solutions adopted by LCs for third-party deposit identification and due diligence

Example 11: Using API and automated name matching tool to facilitate identification of third-party deposits

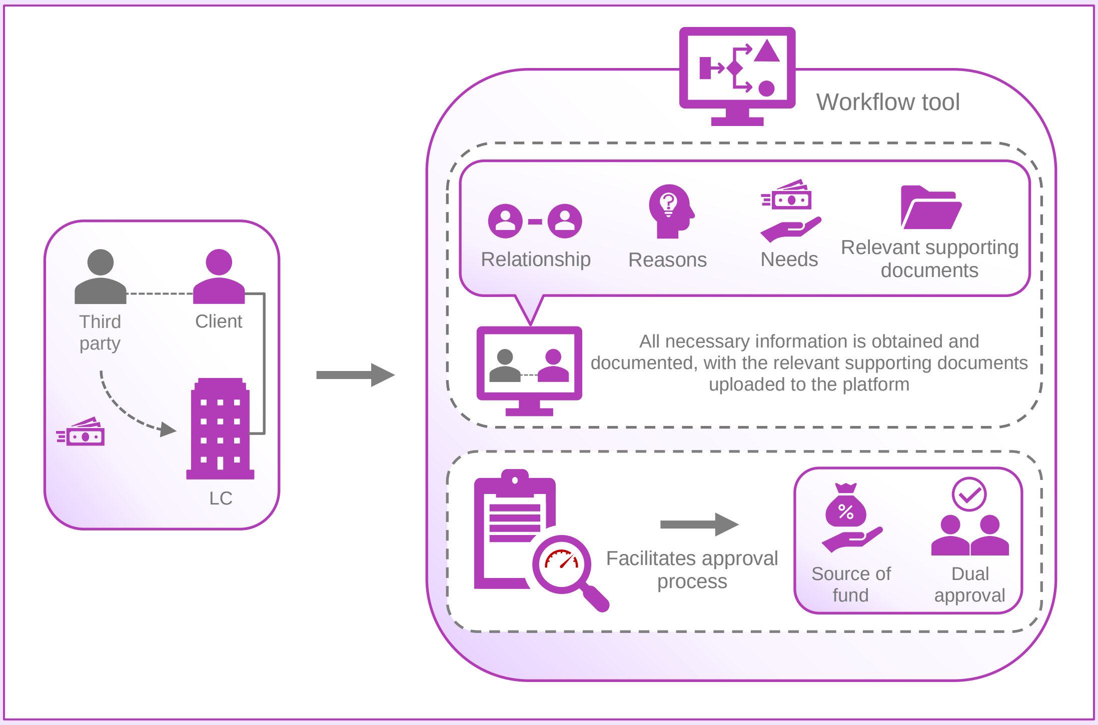

Deposit amount
Depositors' full name
Deposit time
Client deposit information
Bank
Information automatically feeds to LC's system every 30 minutes via API connection
LC
Exact name match
Client A
Depositor
Client B
LC's self-developed automated name matching tool
Bank account
Client deposits funds to LC's designated bank account
Deposited funds are automatically credited to the client's trading account
Trading account

An LC has established API connection with banks to obtain information related to deposits received in its bank accounts including depositors' full names, deposit amount and time. This information would be automatically fed to the LC's system at regular time intervals, such as every 30 minutes, for subsequent name matching.

The LC has developed an automated name matching tool to simplify its comparison of the depositor's name obtained through API connection with banks and the customer's names in the LC's database. If the depositor's name exactly matches with the customer's name, the deposited funds would be automatically credited to the client's trading account as available funds.

In addition to improving efficiency and effectiveness, the LC recognised that this approach has also enhanced customer experience as customers are no longer required to furnish supporting documents for their deposits.

Example 12: Using workflow tool for the performance of third-party deposit due diligence procedures


Third party
Client
LC
Workflow tool
Relationship
Reasons
Needs
Relevant supporting documents
All necessary information is obtained and documented, with the relevant supporting documents uploaded to the platform
Facilitates approval process
Source of fund
Dual approval

An LC has implemented a workflow tool for the performance of third-party deposit due diligence procedures. It has enhanced operational efficiency by eliminating extensive email communication with various stakeholders while providing guided due diligence procedures at the same time.

The workflow tool ensures all necessary information such as the relationship between the third parties and the customers, reasons and needs for third-party deposits, is obtained and documented. The relevant supporting documents obtained are also uploaded to the platform before proceeding to the approval process.

The tool has also incorporated the risk-based element to facilitate the approval process for higher risk situations. This requires additional information regarding the source of funds and mandates dual approval from senior management before releasing the funds.

IV. Responsible adoption of Regtech solutions in the AML/CFT processes

66. This report, including the illustrative use cases of Regtech adoption, has highlighted that Regtech solutions can significantly enhance operational efficiency and the effectiveness of measures in combatting ML/TF. While recognising the benefits, LCs are reminded that they should implement Regtech solutions in a responsible manner, having regard to the four key principles set out below.

A. Governance and accountability

67. In line with the existing requirements, the senior management of an LC is responsible for implementing effective AML/CFT policies, procedures and controls, including any Regtech solutions that have been adopted, to ensure that they can adequately manage the ML/TF risks identified.

68. Where Regtech solution is adopted, an LC is reminded that it remains accountable for discharging its AML/CFT obligations. The LC is therefore expected to include the following in its policies and procedures to ensure that any Regtech solutions adopted are subject to proper governance and oversight:

(a) Conducting proper due diligence and testing on the Regtech solutions to satisfy itself that the solution enables the LC to comply with relevant requirements in an effective manner;

(b) Ensuring the adequacy and effectiveness of the Regtech solutions are subject to regular review, and any issues identified are timely escalated to senior management; and

(c) Ensuring the parameters, thresholds, algorithms and system logics, adopted in the Regtech solutions, including any subsequent adjustments, are properly documented and subject to appropriate level of approval by senior management, while ensuring the approving authorities have sufficient knowledge and expertise to understand the solutions.

B. Ongoing monitoring of Regtech solutions

69. There are no universally applicable Regtech solutions in the market. LCs should 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.

70. When implementing Regtech solutions, LCs are expected to have a demonstrable and thorough understanding of how the solution works, including the underlying technologies employed, and whether the system settings could effectively operate and deliver the intended results, including the appropriateness of the data, variables and decision points for achieving the results.

71. For Regtech solutions involving AI models, LCs are expected to define key principles underlying the model algorithms to achieve the intended outcome. It is also important to have sufficient human oversight to allow for critical evaluation, validation, and correction of AI-generated outputs. For instance, where AI models are adopted in the Regtech solutions to automatically filter out some false positive alerts, LCs are expected to conduct sufficient testing to ensure that this filtering function operates as intended and does not filter out any true hits, including false negative, which warrant further scrutiny.

72. The adequacy, appropriateness and effectiveness of the parameters and thresholds should be subject to independent validation and ongoing monitoring to ensure that they are appropriate to the LC's business operations and context, and function effectively as intended.

C. Data protection and cybersecurity

73. AML/CFT processes involve a substantial amount of customer and transaction data. It is the responsibility of LCs to ensure that the customer and transaction data, systems and networks are subject to adequate and appropriate protection, regardless of whether Regtech solutions are adopted.

74. Various measures are expected to be taken to safeguard personal data from unauthorised access, use or disclosure. These include ensuring that personal data are collected, used, transferred, stored and disposed securely and in compliance with applicable data protection laws and regulations. In addition, LCs are expected to establish cybersecurity measures such as encryption, firewalls and access controls to safeguard their computer systems and networks from cybercrime and cyberattacks. The controls in relation to data protection and cybersecurity measures are expected to be subject to regular review to ensure their effectiveness.

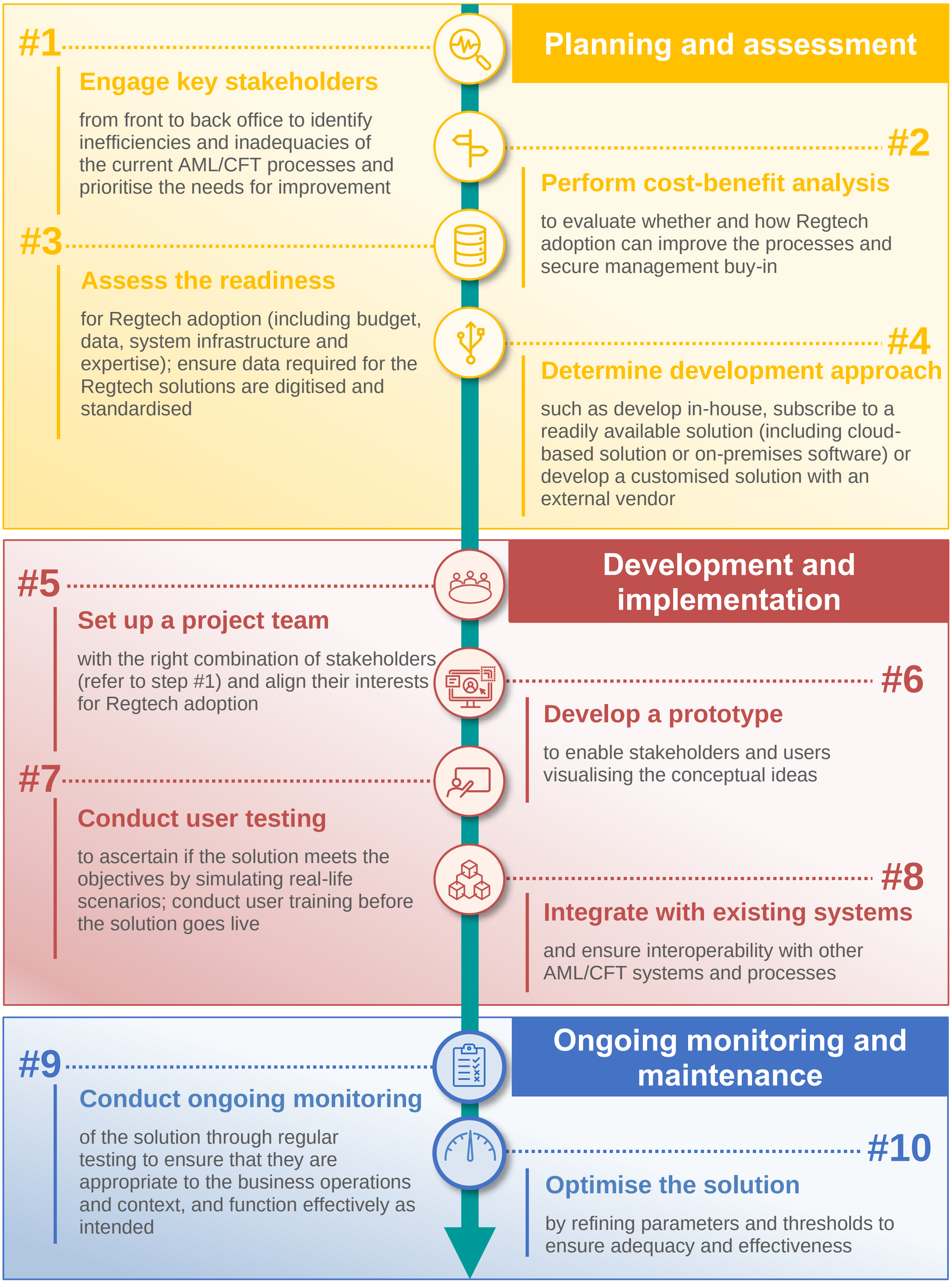
D. Managing risks posed by external vendors

75. When engaging an external vendor for a readily available Regtech solution or developing a customised solution, LCs should be mindful of the risks posed by the external vendor and implement appropriate measures to manage and mitigate any potential risks. LCs are expected to exercise due skill, care and diligence in its selection of the external vendor, having regard to the vendor's track-record and reputation. This includes conducting appropriate due diligence and ongoing monitoring to evaluate whether the external vendor possesses the requisite skills, knowledge, expertise, resources and appropriate controls to deliver and maintain the Regtech solution based on the LC's needs and specifications.

76. In addition, due considerations should be given to the external vendor's controls related to data governance and protection as well as cybersecurity measures. LCs are also expected to establish appropriate contingency plans to ensure their AML/CFT systems and controls remain resilient in the event of disruption of the Regtech solutions such as unplanned system outage.

77. In addition to the aforementioned key principles, LCs are also advised to refer to the Regtech adoption roadmap set out in the Appendix of this report. The roadmap provides a concise overview of the key steps identified through the SFC's analysis of case studies on Regtech adoption by selected LCs.

Regtech adoption roadmap



Planning and assessment

#1

Engage key stakeholders

from front to back office to identify inefficiencies and inadequacies of the current AML/CFT processes and prioritise the needs for improvement

#2

Perform cost-benefit analysis

to evaluate whether and how Regtech adoption can improve the processes and secure management buy-in

#3

Assess the readiness

for Regtech adoption (including budget, data, system infrastructure and expertise); ensure data required for the Regtech solutions are digitised and standardised

#4

Determine development approach

such as develop in-house, subscribe to a readily available solution (including cloud-based solution or on-premises software) or develop a customised solution with an external vendor

Development and implementation

#5

Set up a project team

with the right combination of stakeholders (refer to step #1) and align their interests for Regtech adoption

#6

Develop a prototype

to enable stakeholders and users visualising the conceptual ideas

#7

Conduct user testing

to ascertain if the solution meets the objectives by simulating real-life scenarios; conduct user training before the solution goes live

#8

Integrate with existing systems

and ensure interoperability with other AML/CFT systems and processes

Ongoing monitoring and maintenance

#9

Conduct ongoing monitoring

of the solution through regular testing to ensure that they are appropriate to the business operations and context, and function effectively as intended

#10

Optimise the solution

by refining parameters and thresholds to ensure adequacy and effectiveness