Smart tips for

Private Banking

Anti-Money Laundering and Counter-Financing of Terrorism Measures

Establishment of Source of Wealth and Source of Funds

Customer due diligence (CDD) measures are not only for meeting regulatory requirements, but also help drive private banking relationships and understand clients' needs for providing better services.

What is Source of Wealth?

Source of wealth refers to the **origin** of an individual's entire body of wealth (i.e. total assets). This information will usually give **an indication** as to the size of wealth the customer would be expected to have, and **a picture** of how the individual acquired such wealth.

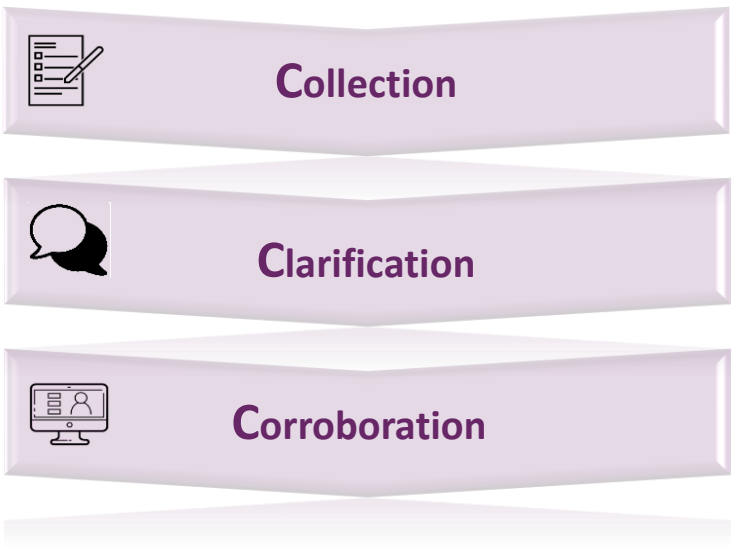
What is Source of Funds?

Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship **between an individual and the Authorized Institution (AI)** (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

Establish ≠ Verify

Establishing source of wealth and source of funds does not mean verifying all the information for accuracy. The HKMA's regulatory expectation is for AIs to take reasonable measures commensurate with the assessed risks.

The "3-C" approach



Establishment of Source of Wealth and Source of Funds

Do

✓ Obtain a broad picture of the customer's total wealth and how such wealth was acquired

✓ Focus on asking questions that can help assess legitimacy or reasonableness of customer's wealth and the source of funds

✓ Check against publicly available information (e.g. property registers, land registers or news articles) to corroborate some key information provided by the customer

✓ Ask for verification or validation documents from customers only when there is doubt on the veracity of specific information provided by the customer

Don't

✗ Collect excessive information from the customer (e.g. bank statements or employment records dating back decades)

✗ Verify every piece of source of wealth information provided by the customer

✗ Make unreasonable repeated requests for additional information prolonging account opening

✗ Apply the same checklist to every customer mechanically without taking into account individual circumstances and information already collected

Good Practice 1

- Customer X is a co-founder and executive chairman of a listed company and has been assigned a low risk rating by Bank A when opening a PB investment account.
- Customer X indicated that his wealth has been generated mostly through the listed company.
- In establishing Customer X's source of wealth, rather than requesting the customer to provide documentary proofs of his declaration, Bank A conducted an internet search and made reference to available information in the public domain (e.g. annual report and online news article), as well as calculating the value of the company and the customer's personal wealth based on performance of the share prices on the internet, and corroborated information obtained from Customer X and public sources.

Good Practice 2

- Customer Y is a personal investment company ultimately owned by 3 beneficial owners (BOs).
- Customer Y's PB investment account has been assigned a high risk rating according to the policy of Bank B.
- In corroborating Customer Y's source of wealth, Bank B verified the positions held by the BOs through online searches and pubic information (e.g. company website), properly documented the BOs' journey to wealth, and estimated their annual income and investment return using a prudent approach, with the basis documented, to arrive at the net worth. Proceeds from sales of shares and properties are supported by market research and land searches.

Ongoing Monitoring

Ongoing monitoring is a dynamic process. The way private banking relationships are managed, with personalised services provided by dedicated relationship managers, makes many innovative ways to conduct ongoing monitoring possible. Ongoing monitoring is more than ticking the box or filling a checklist periodically.

Do

- ✓ Make the best use of day-to-day communication to keep customer profiles up-to-date
- ✓ Set the timeframes of periodic CDD reviews for different customers according to their risk profiles
- ✓ Focus on areas where there are updates during periodic CDD review
- ✓ Monitor customer transactions through relationship management, and clarify with the customers where appropriate
- ✓ Remain vigilant to suspicious indicators and red flags when monitoring customers' account activities especially those involving third-party transfers

Don't

- ✗ Re-do CDD during periodic reviews (e.g. disregard information provided by the customer previously and ask for the same information all over again)
- ✗ Overly rely on rule-based transaction monitoring and seek clarification from the customer a long time after the transaction was conducted
- ✗ Inquire into every single transaction carried out by customers without taking into account the customer's background and any risk indicators involved in the transaction

Good Practice 3

- Under Bank C's customer risk assessment framework, a majority **(~90%)** of the corporate customers were automatically assigned a high risk rating without proper assessment.
- As enhanced monitoring on a large population of high risk customers was unsustainable, Bank C engaged external consultants to help revamp its customer risk assessment framework including the risk category and CDD review cycle.
- Under the revised framework, the number of high risk corporate customers was reduced significantly with only around **30%** subject to annual CDD review, and have helped relieve pressure on Bank C's AML compliance significantly to focus on effectiveness and intended outcomes.

Good Practice 4

- Bank D provided standardised CDD review forms for its staff to conduct periodic reviews. However, the forms were long (~15 pages) and required staff to collect lots of information from customers all over again.
- To improve efficiency and customer experience, Bank D subsequently updated its process to rely more on information obtained during ongoing customer communication (e.g. call reports) and focus on areas where there are updates. This helps significantly reduce the amount of information to be collected and time taken for periodic reviews.

AML Regtech Adoption

All banks, including private banks, are encouraged to explore AML Regtech. The HKMA supports the use of technologies for AML/CFT.

Do

- ✓ Explore opportunities to use Regtech to offer better customer experience (e.g. using reliable digital identification systems such as iAM Smart)
- ✓ Provide different delivery channels for customer engagement (e.g. video conferencing)
- ✓ Understand the systems and processes deployed and support with skilled expertise
- ✓ Ensure accurate, complete and relevant data through regular assurance testing on data quality and lineage
- ✓ Implement effective management oversight on AML Regtech adoption

Don't

- ✗ Ignore problems of legacy architecture
- ✗ Deploy off-the-shelf systems provided by external vendors or head office without fully taking into account local circumstances
- ✗ Devote insufficient resources to Regtech projects

Good Practice 5

- Bank E has launched an initiative to leverage a digitalised platform with Regtech tools. When a prospective customer uploads his identity document, the system automatically assists staff to authenticate the document, including running through a comprehensive list of security features. This helps improve efficiency and automate processes, freeing staff for higher-value activities.
- A list of control checkpoints is used to ensure all the data points are captured.
- The digitalised platform facilitates interaction with the prospective customer via high quality video conferencing. To mitigate impersonation risk, Bank E also applies appropriate risk mitigating controls.
- Better organised data and more analytical tools help Bank E's staff to understand and target higher ML risk areas.

Good Practice 6

- Bank F uses a centralised, automated platform with artificial intelligence to consolidate its CDD processes, including corroborating source of wealth and identifying hidden source of wealth based on various sources; and automatically generate name screening and adverse news search results.
- With the adoption of this auditable artificial intelligence, false positive cases decreased significantly.