❖ **Understand What is KYC Identify**

What is KYC?

Know Your Customer (KYC) procedures are a critical function to assess customer risk and a legal requirement to comply with Anti-Money Laundering (AML) laws. Effective KYC involves knowing a customers identity, their financial activities and the risk they pose.

Do you know your customer? At any rate, you ought to. If you're a financial institution (FI), you could face possible fines, sanctions, and reputational damage, if you do business with a money launderer or terrorist. More importantly, KYC is a fundamental practice to protect your organization from fraud and losses resulting from illegal funds and transactions.

"KYC" refers to the steps taken by a financial institution (or business) to:

- Establish customer identity
- Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate)
- Assess money laundering risks associated with that customer for purposes of monitoring the customer's activities

To create and run an effective KYC program requires the following elements:

1) Customer Identification Program (CIP)

How do you know someone is who they say they are? After all, identity theft is widespread, affecting over 16.7 million US consumers and accounting for 16.8 billion dollars stolen in 2017. For obliged entities, such as financial institutions, it's more than a financial risk – it's the law.

In the US, the CIP mandates that any individual conducting financial transactions needs to have their identity verified. Provisioned in the Patriot Act, the CIP is designed

to limit money laundering, terrorism funding, corruption and other illegal activities. Other jurisdictions have similar provisions; over 190 jurisdictions around the world have committed to recommendations from the Financial Action Task Force (FATF), a pan-government organization designed to fight money laundering. These recommendations include identity verification procedures.

The desired outcome is that obliged entities accurately identify their customers.

A critical element to a successful CIP is a risk assessment, both at the institutional level and at the level of procedures for each account. While the CIP provides guidance, it's up to the individual institution to determine the exact level of risk and policy for that risk level.

The minimum requirements to open an individual financial account are clearly delimited in the CIP:

- Name
- Date of birth
- Address
- Identification number

While gathering this information during account opening is sufficient, the institution must verify the identity of the account holder "within a reasonable time." Procedures for identity verification include documents, non-documentary methods (these may include comparing the information provided by the customer with consumer reporting agencies, public databases, among other due diligence measures), or a combination of both.

These procedures are at the core of CIP; as with other Anti-Money Laundering (AML) compliance requirements, these policies shouldn't be followed willy-nilly. They need to be clarified and codified to provide continued guidance to staff, executives, and for the benefit of regulators.

The exact policies depend on the risk-based approach of the institution and may consider factors such as:

- The types of accounts offered by the bank
- The bank's methods of opening accounts
- The types of identifying information available
- The bank's size, location, and customer base, including the types of products and services used by customers in different geographic locations

2) Customer Due Diligence

For any financial institution, one of the first analysis made is to determine if you can trust a potential client. You need to make sure a potential customer is trustworthy; customer due diligence (CDD) is a critical element of effectively managing your risks and protecting yourself against criminals, terrorists, and Politically Exposed Persons (PEPs) who might present a risk.

There are three levels of due diligence:

- **Simplified Due Diligence** ("SDD") are situations where the risk for money laundering or terrorist funding is low and a full CDD is not necessary. For example, low value accounts or accounts.
- **Basic Customer Due Diligence** ("CDD") is information obtained for all customers to verify the identity of a customer and asses the risks associated with that customer.
- **Enhanced Due Diligence** ("EDD") is additional information collected for higher-risk customers to provide a deeper understanding of customer activity to mitigate associated risks. In the end, while some EDD factors are specifically enshrined in a country's legislations, it's up to a financial institution to determine their risk and take measures to ensure that their customers are not bad actors.

Some practical steps to include in your customer due diligence program include:

- Ascertain the identity and location of the potential customer, and gain a good understanding of their business activities. This can be as simple as locating documentation that verifies the name and address of your customer.
- When authenticating or verifying a potential customer, classify their risk category and define what type of customer they are, before storing this information and any additional documentation digitally.
- Beyond basic CDD, it's important that you carry out the correct processes to ascertain whether EDD is necessary. This can be an ongoing process, as existing customers have the potential to transition into higher risk categories over time; in that context, conducting periodic due diligence assessments on existing customers can be beneficial. Factors one must consider to determine whether EDD is required, include, but are not limited to, the following:

- Location of the person
- Occupation of the person
- Type of transactions
- Expected pattern of activity in terms of transaction types, dollar value and frequency
- Expected method of payment

- Keeping records of all the CDD and EDD performed on each customer, or potential customer, is necessary in case of a regulatory audit.

3) Ongoing Monitoring

It's not enough to just check your customer once, you need to have a program to monitor your customer on an ongoing basis. The ongoing monitoring function includes oversight of financial transactions and accounts based on thresholds developed as part of a customer's risk profile.
Depending on the customer and your risk mitigation strategy, some other factors to monitor may include:

- Spikes in activities
- Out of area or unusual cross-border activities
- Inclusion of people on sanction lists
- Adverse media mentions

There may be a requirement to file a Suspicious Activity Report (SAR) if the account activity is deemed unusual.
Periodical reviews of the account and the associated risk are also considered best practices:

- Is the account record up-to-date?
- Do the type and amount of transactions match the stated purpose of the account?
- Is the risk-level appropriate for the type and amount of transactions?

In general, the level of transaction monitoring relies on a risk-based assessment.