Anti-money laundering (AML) & Countering financing of terrorism (CFT)

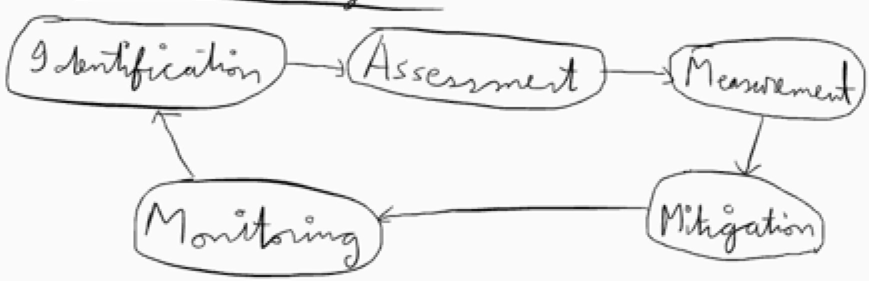
Objectives

→ Prevent growth of terrorism & support the Government's efforts towards the same
→ Preserve the integrity of the banking system

* Risks of lack of ML/FT risk mgmt policies

→ Fines & penalties
→ Loss of reputation
⇓
Loss of business → Even threaten the viability & survival of the bank
→ Diversion of time & money from business to damage control activities

*. Risk management



Identification

→ Understanding of the ML/FT risks
→ Developing a taxonomy or register of risks

Assessment

→ Identify areas of the business where these risks emerge
→ Brainstorm on how the same can be effectively managed

Mitigation

→ Development of policies, procedures, systems to minimize the risk occurrence

Monitoring

→ Ensure compliance with policies
→ Review & update of policies & processes on a regular basis depending on emerging practices

3 lines of defense

1) First line : Business units (customer facing roles)
→ Understand & comply with ML/FT RM policy
→ undertake proper due diligence as required by the policy

2) Second line : AML/CFT officer
→ Ensure implementation & compliance of the ML/FT RM policy across the organization
→ Ensure compliance with national laws & regulator guidelines
→ Report to the Board & senior mgmt on suspicious activity or transactions

3) Third line : Internal audit
→ Review & test compliance with ML/FT RM policy on a sample basis
→ Suggest improvements in existing process & controls

*. 4 aspects to be considered

1) Customer acceptance

→ Segregate customers into risk buckets say low, medium, high to ascertain the level of due diligence to be carried out

→ Parameters for segregating could be source of income, purpose of opening account, nature of business, etc.

Examples of low risk

→ Salaried people
→ Small balances & infrequent transactions
→ Govt. entities or govt. companies

Examples of high risk

→ Large balances
→ Frequent cross-border transactions
→ NRIs, NGOs (specially those with foreign contributions), HNIs, shell companies, Politically exposed Persons (PEPs)

RBI guidelines

→ No benami account
→ Parameters / risk indicators for customer segregation to be clearly defined
→ Documentation based on risk category
→ No account to be opened without proper due diligence
→ Check that customer profile does not match sanctioned list of people

2.) Customer identification

→ Establishing the identity of the person in whose name the accant is opend

→ Can be ascertained through ID proof such as passport, license, etc

RBI guidlines

→ List of documents which are acceptable

→ KYC to be performed regularly (every 2 years for high & medium risk & 5 years for low risk)

→ For dependants address proof in the name of breadwinner is acceptable

3.) Monitoring of transactions

→ Triggers or warning indicators to identify suspicious accant activity

→ Prepare STR (Suspicious Transaction Report) for doubtful transactions and submit to Financial Intelligence Unit (FIU) for further investigation

→ Periodically run customer database against sanctions list

RBI guidelines

→ Review risk categorization of customers every 6 months

→ Establish parameters or indicators for monitoring transactions