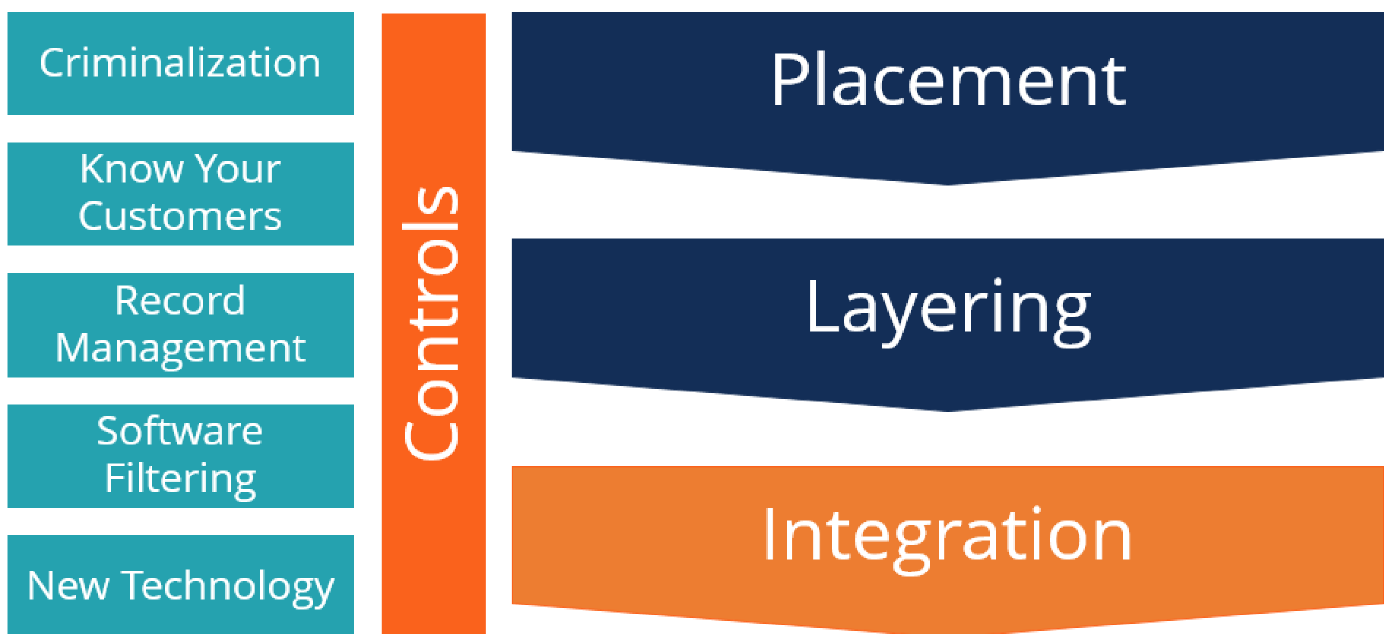
Anti-Money Laundering (PUN004)

Money laundering refers to the process of taking illegally obtained money and making it appear to have come from a legitimate source. It involves putting the money through a series of commercial transactions in order to "clean" the money. For example, money may be placed in a business and disguised as sales revenue in order to camouflage its origin. Money laundering is illegal in itself.

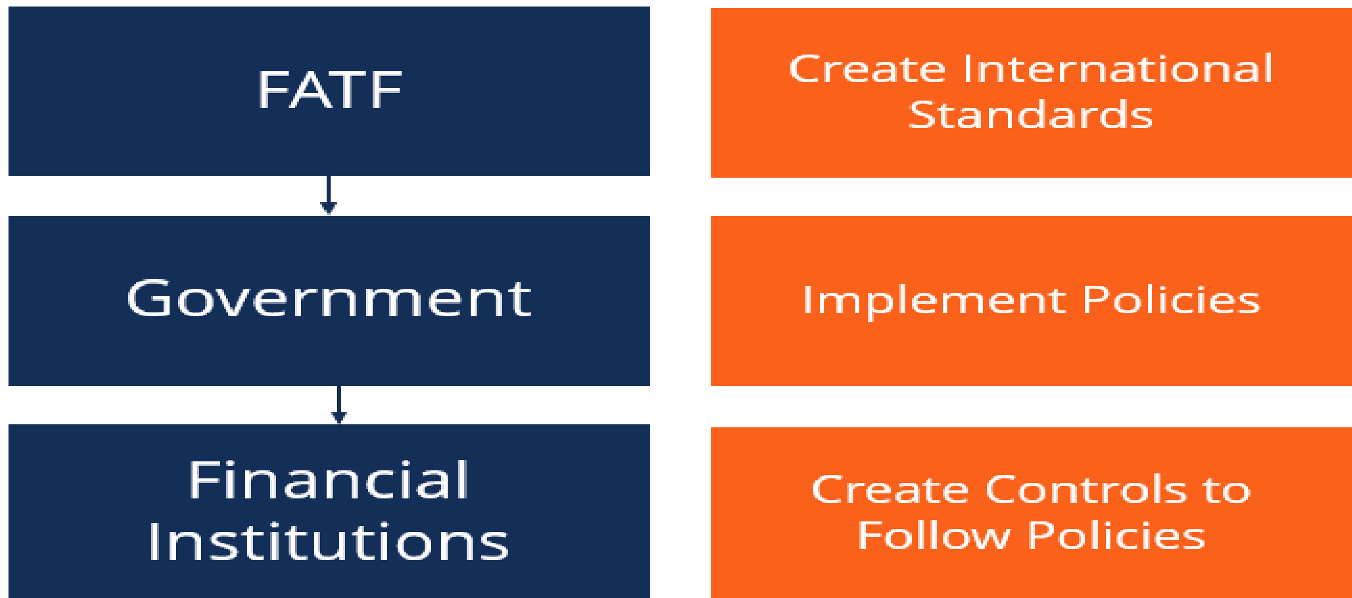
Process: The figure below shows the three steps in money laundering and some of the controls that are used to prevent it. Money laundering is carried out through **placement** in a financial institution carrying out a series of transactions to disguise its original source (layering) and obtaining/using the cleaned money (integration).

Layering: It is to make it more difficult to detect and uncover a laundering activity. It is meant to make the trailing of illegal proceeds difficult for the law enforcement agencies. The known methods are, Cash converted into Monetary Instruments - Once the placement is successful within the financial system by way of a bank or financial Institution, the proceeds can then be converted into monetary instruments. This involves the use of banker's drafts and money orders. Material assets bought with cash then sold - Assets that are bought through illicit funds can be resold locally or abroad and in such a case the assets become more difficult to trace and thus seize.



The first anti-money laundering structures came about with the Financial Action Task Force (FATF). It ensures that international standards are put in place to prevent money laundering. Since the 2001 terrorist attacks, the FATF now also includes terrorist surveillance in an effort to mitigate terrorist financing. Recently, cryptocurrency has come under scrutiny, as it provides anonymity to its users. This has facilitated a lower-risk method for criminals to go about their transactions.

Financial institutions are held to high standards with regards to following procedures to identify money laundering. All bank employees are trained to some degree to identify and monitor suspicious customer activity. Larger financial institutions will also have dedicated departments to track fraud and money laundering. Many of the institutions put in place a "know your client" measure, which can help flag suspicious transactions based on particular clients. Transactions and processes at financial institutions are recorded extensively so that law enforcement can trace the crimes back to the source. While such institutions are legally obligated to follow anti-money laundering regulations as they relate to the country they operate in, not all agree with them. Implementing the policies are often costly and ineffective, and the net benefit of having them in place often comes into question.



Controls:

Criminalization: Many governments, financial institutions, and businesses impose controls to prevent money laundering. The first is criminalization by the government. The United Nations Convention Against Transnational Organized Crime has set forth guidelines that help governments to prosecute individuals involved in money laundering schemes.

Know Your Customers: Financial institutions must also have "know your customer" policies in place to help prevent money laundering. This involves monitoring the activity of clients and understanding the types of transactions that should raise red flags. Financial institutions are required to report suspicious activity to a financial investigation unit.

Record Management and Software Filtering: Financial institutions and businesses also keep detailed records of transactions and implement software that can flag suspicious activity. Customer data can be classified based on varying levels of suspicion, and transactions denied if they meet certain criteria.

Holding Period: Many banks require deposits to remain in an account for a designated number of days (usually around five). This holding period helps manage risk associated with money being moved through banks to launder money.

New Technology: The technology used to identify suspicious activity linked to money laundering continues to evolve and become more accurate. Technologies, such as AI and Big Data software, allow these systems to become more sophisticated.

As per RBI, the Customer Acceptance Policy (CAP) Banks should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank. No account is opened in anonymous or fictitious/benami names, Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III); customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs as explained in Annex 1) may, if considered necessary, be categorised even higher, documentation requirements and other information to be collected in respect of different categories of customers depending on.

A relevant employee should be aware of all listed options Le policies and procedures put in place to prevent money laundering, procedures put in place to prevent money laundering and KYC/AML guidelines issued by the RBI. As per new norms, full KYC exercise will be required to be done at least every 10 years for low risk and at least every 8 years for medium risk individuals and entities. While for the high-risk individuals and entities, it should be done in at least every 2 years. As per new norms, full KYC exercise will be required to be done at least every 10 years for low risk and at least every 8 years for medium risk Individuals and entities. While for the high-risk individuals and entities, it should be done in at least every 2 years.

As per RBI, Assessment and Monitoring of Risk In terms of paragraph 2 of Annex vi of the Master Circular DNBC(PD)CC No 231/03.10.42/2011-12 dated July 01, 2011 on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002, NBFCs are required to prepare a risk profile of each customer and apply enhanced due diligence measures on higher risk customers. Some illustrative examples of customers requiring higher due diligence have also been provided in the paragraph under reference. Further, paragraph 5 of Annex vi of the Master Circular requires NBFCs to put in place policies, systems and procedures for risk management keeping in view the risks involved in a transaction, account or banking/business relationship. The Government of India had constituted a National Money Laundering/Financing of Terror Risk Assessment Committee to assess money laundering and terror financing risks, a national AML/CFT strategy and institutional framework for AML/CFT in India. Assessment of risk of Money Laundering/Financing of Terrorism helps both the competent authorities and the regulated entities in taking necessary steps for combating ML/FT adopting a risk-based approach. This helps in judicious and efficient allocation of resources and makes the AML/CFT regime more robust.

The Committee has made recommendations regarding adoption of a risk-based approach, assessment of risk and laundering and terror financing risks, a national AML/CFT strategy and institutional framework for AML/CFT in India. Assessment of risk of Money Laundering/Financing of Terrorism helps both the competent authorities and the regulated entities in taking necessary steps for combating ML/FT adopting a risk-based approach. This helps in judicious and efficient allocation of resources and makes the AML/CFT regime more robust. The Committee has made recommendations regarding adoption of a risk-based approach, assessment of risk and putting in place a system which would use that assessment to take steps to effectively counter ML/FT.

The recommendations of the Committee have since been accepted by the Government of India and needs to be implemented. As per RBI, Intra-bank Deposit Accounts Portability It has been brought to our notice that some banks are insisting on opening of fresh accounts by customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Such insistence on opening of fresh account or making the customer undergo full KYC process again causes inconvenience to them resulting in poor customer service. It is not reasonable in view of the fact that most bank branches are now on CBS and KYC records of a particular customer can be accessed by any branch of the bank, 2. Banks are advised that KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer should be allowed to transfer his account from one branch to another branch without restrictions. In order to comply with KYC requirements of correct address of the person, fresh address proof may be obtained from him/her upon such transfer by the transferee branch. It may be noted that instructions regarding periodical update of KYC data in terms of para 2.4(e) and those on maintenance of records of identity and transaction in terms of para 2.21(il) of our Master circular DBOD AML BC. No.2/14.01.001/2009-10 dated July 01, 2011 remain unchanged and banks will be required to carry out the update at prescribed intervals as also maintain records of transactions and verification of identity as prescribed.

The Prevention of Money Laundering Act (PMLA) 2002 defines the offence of Money Laundering as Engaging directly or indirectly in a transaction that involves property, that is proceeds of crime (or) derived from proceeds of crime (or) knowingly receiving, possessing, concealing, disguising, transpiring, converting, disposing off within the territories of India, removing from or bringing into the territory of India the property that is proceeds of crime. As per RBI, Banks/FIS should exercise on going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds. The Board of Directors should ensure that an effective AML/CFT programme is in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters. In addition, the following may also be ensured for effectively implementing the AML/CFT requirements:
1. Using a risk-based approach to address management and mitigation of various AML/CFT risks.
il Allocation of responsibility for effective implementation of policies and procedures.
ill. Independent evaluation by the compliance functions of bank/FI's policies and procedures, including legal and regulatory
requirements
Iv. Concurrent/internal audit to verify the compliance with KYC/AML policies and procedures.
v. Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

Firms must comply with the Bank Secrecy Act and its implementing regulations (Anti-Money Laundering rules"). The purpose of the AML rules is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing, such as securities fraud and market manipulation. Prevention of Money Laundering

Act, 2002 is an Act of the Parliament of India enacted by the NDA government to prevent money-laundering and to provide for confiscation of property derived from money-laundering, PMLA and the Rules notified there under came into force with effect from July 1, 2005. Government of India, Notification dated December 16, 2010. The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities within the overall Group AML Policy framework, the key AML objectives of the Bank are: To prevent the Bank's business channels/products/services from being used as a channel for ML. To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Bank.

Thank You...