KYC/AML Compliance Requirements by Indian Financial Service Providers and Suggested Solutions

The KYC/AML comprehensive instructions are issued by Reserve Bank of India and if these instructions are followed in proper spirit by the financial institutions, the system and procedures would operate effectively. Unfortunately, the business becomes the prime focus of all activities and as a consequence KYC/AML is either not followed or at times ignored. Business takes priority over compliance. In this article, an attempt is made to highlight the cardinal principles of KYC/AML and how these can be implemented by the financial institutions by adhering to the instructions of regulators through technological procedures. Read on to know more……

CA. Durgaprasad Khatri* and Mr. Siddhartha Kher **

(* The author is a member of the Institute. **The author is a Certified Fraud Examiner. The authors can be reached at khatri.durgaprasad@gmail.com.)

KYC/AML is taken seriously by the Regulators all over the world. In India also, timely changes are made in the Prevention of Money Laundering Act 2002 (PMLA), the recent amendment to the act carried out in 2012 expanding the definition, scope and introduction of stringent action against defaulters. All major institutions rendering financial services are covered by PMLA and these

include Banks, Insurance Companies, Depository Participants, Brokers including sub-brokers, PMS service providers, Mutual Funds, Distributors of Mutual Fund Products, Asset Management Companies, Alternative Investment Fund, Joint Ventures, Wealth Advisors and other service providers.

Financial Action Task Force (FATF) is a powerful inter-governmental body whose purpose is development and promotion of international standards to combat money laundering and terrorist financing. India is a member of FATF and legitimately bound to adhere to the FATF guidance which is based on the risk-based approach to combating money laundering and terrorist financing.

The FATF principles are propagated by Reserve Bank of India in its Master Circular–Know Your Customer (KYC) norms/Anti Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligation of banks and financial institutions under PMLA, 2002. This RBI circular in detail covers the principles to be followed by banks and financial institutions in relation to KYC and AML/CFT. Securities and Exchange Board of India (SEBI) has also articulated FATF principles in its circular on KYC. Banks and the financial service providers need to decide the methodology to be followed to ensure that the laid down principles by RBI are empirically implemented.

In order to control the anti-money laundering activities, RBI has emphasised that the Risk-Based Approach should be put in practice while rendering the financial services to its customers. Customer Due Diligence/Know Your Customer is the first step that has to be put in the system and procedures of the Bank or any entity rendering financial services. Knowing the customer means to know customer business, customer financial status and customer intention to operate the transactions. The bank should be fully familiar with the business of customer and understand the activities carried out by the customer. This is fundamental to KYC for onboarding the customer before commencement of financial relationship. The financial institution's systems and procedures should include:

- Identify and verify the identity of each customer on a timely basis– Proof of identity and proof of address

In order to control the anti-money laundering activities, RBI has emphasised that the Risk-Based Approach should be put in practice while rendering the financial services to its customers. Customer Due Diligence/Know Your Customer is the first step that has to be put in the system and procedures of the Bank or any entity rendering financial services.

- Take reasonable risk-based measures to identify and verify the identity of any beneficial owner– where owner of funds is other than the person operating the account i.e. high risk
- Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions– this data would decide the level of risk.

The above process will determine the level of risk in opening the bank account and operating transactions. Based on the facts and circumstances of the customer, the type of business being conducted and geographies where dealings are done, the risk assessment will have to be done. Greater the comfort, lesser would be the risk e.g., account opening of a reputed Listed Company, Government Department, Large Financial Institutions recognised by RBI etc. On the other hand, for a customer where beneficial owner is other than the account holder or request for opening the account has come from Politically Exposed Person, the level of risk will be high and as such enhanced due diligence will have to be followed. The risk based approach would include:

- A standard level of due diligence, to be applied to all customers.
- The standard level being reduced in recognised lower risk scenarios, such as Public Listed Companies, Large Financial Institutions recognised by RBI, Individuals whose main source of income is salary or pension.
- An increased level of due diligence in respect of those customers that are determined to be of higher risk. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher

risk, such as politically exposed persons, dealing in gems and jewellery etc.

Transaction Monitoring and Investigation

The degree and nature of monitoring by a financial institution would depend on the size of the financial institution, the AML/CFT risks that the institution has, the monitoring method being utilised (manual, automated or combination of both), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, financial institutions must recognise that not all transactions, accounts or customers will be monitored in the same way. The mechanism of monitoring will depend on the assessed risks associated with the customer, the products or services being used by the customer and the location of the customer and the type of transactions. Monitoring methodologies and processes also need to take into account the quality resources of the financial institution.

The principle of monitoring in a risk-based system is to respond to enterprise-wide issues based on each financial institution's analysis of its major risks. Risk weights are assigned considering the facts and circumstances of the case and these should be comprehensively explained in the risk manual of entity and adequately documented in the account opening process.

Monitoring under a risk-based approach allows a financial institution to create monetary or other thresholds below which an activity would not be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis, to determine adequacy for the risk levels established. Financial institutions should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented.

Suspicious Transaction Analysing, Reviewing, Finalising and Reporting

On establishing client onboarding the next step is to scrutinise the transactions. The reviewing and reporting of suspicious transactions is critical information to combat money laundering, terrorist financing and other financial crimes. The first step is alerts are generated and analysed and then reporting is done to Financial Intelligence Unit (FIU). The process of correct parameters to be configured for generating alert is key to the objective of monitoring suspicious transactions. Parameters set for generating alerts should be well planned and carefully designed or else it would result in "garbage in garbage out" and will not serve the purpose. Alerts does not mean reporting to be done, these alerts are to be analysed and then decision to be taken whether to report to FIU. This is like the task of spotting relevant out of irrelevant transactions.

Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of suspicious activity under these circumstances is not applicable. For example, Cash Transaction Reporting (CTR) mandated by FIU.

A risk-based approach is, however, appropriate for the purpose of identifying suspicious activity. For example, by directing additional resources a those areas a financial institution should address these identified high-risks. A financial institution should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions. This can be achieved through periodical independent internal audits.

Training and Understanding

It is imperative for financial institutions to provide AML/CFT training to all relevant employees at regular intervals. This would cover employees facing the customers, promoting the financial institution products, back office staff and other support staff. The record of all the training imparted has to be maintained and feedback to be obtained from participants about their understanding of the subject and all feedbacks received should be scrutinised to take corrective action. It should be ensured that AML/CFT training enables employees to:

I. understand the relevant legislation relating to money laundering, including provisions of Prevention of Money Laundering Act 2002,

It is imperative for financial institutions to provide AML/CFT training to all relevant employees at regular intervals. This would cover employees facing the customers, promoting the financial institution products, back office staff and other support staff.

The framework of internal checks and balances should provide for regular review of the risk assessment and management processes, taking into account the environment within which the financial institution operates and the activity in its market place.

recently pronounced cases and judgments of High Court and Supreme Court on AML/CFT;

II. understand its policies, procedures, controls and systems related to money laundering and any changes to these;

III. recognise and deal with transactions and other activities which may be related to money laundering;

IV. understand the types of activity that may constitute suspicious activity in the context of the business of customer;

V. be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

VI. understand the roles and responsibilities of Employees in combating money laundering, and line of reporting to compliance officer or principal officer;

VII. understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in laid down procedures.

Ensure that its AML training:

i. is appropriately tailored to the Relevant Person's activities, including its products, services, customers, distribution channels, business partners, level and complexity of its transactions; and

ii. indicates the different levels of money laundering risk and vulnerabilities associated.

Internal Checks, Balances and Controls

In order for financial institutions to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the financial institutions. Chairman and Managing Director and other Senior management are ultimately responsible for ensuring that a financial institution maintains timely and an effective internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and its engagement in AML is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the financial institution's policies, procedures and processes designed to limit and contain risks.

In addition to other compliances, internal controls, the nature and extent of AML/CFT controls will depend upon a number of factors, including:

- The nature, scale and complexity of a financial institution's business.
- The diversity of a financial institution's operations, including geographical diversity.
- The financial institution's customer, product and activity profile.
- The distribution channels used.
- The volume and size of the transactions.
- The degree of risk associated with each area of the financial institution's operation.
- The extent to which the financial institution is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non face to face access.

The framework of internal checks and balances should:

- Provide increased focus on a financial institution's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
- Provide for regular review of the risk assessment and management processes, taking into account the environment within which the financial institution operates and the activity in its market place.
- Principal Officer at senior management level responsible for managing AML/CFT compliance.
- Establish an AML/CFT compliance function and review programme.
- Ensure that adequate controls are in place before new products are introduced.
- Inform Audit Committee of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.

- Provide for programme continuity despite changes in management or employee composition or structure.
- Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence policies, procedures and processes.
- Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals above a threshold.
- Enable the timely identification of reportable transactions through generation of alerts and its analysis and ensure accurate and timely filing of reports to Financial Intelligence Unit (FIU), New Delhi.
- Incorporate AML/CFT compliance into job descriptions and performance appraisal of appropriate personnel.
- Provide for appropriate training to be given to all relevant staff at regular intervals and record to be maintained for the same.
- For groups, to the extent possible, there should be a common control framework.

Many software companies can sell an institution dedicated systems to combat laundering, while some organisations have internally generated electronic systems. Before designing your AML compliance program or purchasing new technology, review the feasibility, costs and benefits to be derived from each course of action.

Chairman and Managing Director and Senior Management would need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of the financial institution. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, forensic consultants or other qualified parties who are not involved in the implementation or operation of the financial institution's AML/CFT compliance programme. The testing should be risk-based (focusing attention on higher-risk customers, products and services); should evaluate the adequacy of the financial institution's overall AML/CFT programme; and the quality of risk management for the financial institution's operations, departments and subsidiaries; include comprehensive procedures and testing; and cover all activities.

Technological Solution for Compliance

Almost all financial institutions would agree that anti-money laundering compliance is nearly impossible without some help from technology. The sheer volume of regulations make manual compliance difficult if not impossible. Many institutions have computer systems to automate their compliance activities, while a few still undertake their efforts manually. Although technology forms one of a number of components in an overall AML solution, good technology will equip organisations with improved defences in the fight against financial crime by providing:

- **Transaction monitoring:** scanning and analysing data for potential money laundering activity.
- **Watch list filtering:** screening new accounts, existing customers, beneficiaries and transaction counterparties against terrorist, criminal and other blocked-persons' watch lists.
- **Automation of regulatory reporting:** filing suspicious transaction reports (STRs), currency transaction reports (CTRs), or other regulatory reports with the government.
- **A detailed audit trail:** demonstrates compliance efforts to regulators.

Many software companies can sell an institution

dedicated systems to combat laundering, while some organisations have internally generated electronic systems. Before designing your AML compliance program or purchasing new technology, review the feasibility, costs and benefits to be derived from each course of action.

Most institutions seek a partner with a longstanding commitment to stay ahead of the rapidly changing regulatory landscape and with a track record that reflects flexibility, agility and urgency in delivering features that improve clients' efficiency in monitoring the right transactions and investigating the right clients. Ideally, the system must be flexible, fast and efficient to deploy over multiple branches. It should allow the institution to navigate seamlessly around client relationships, accounts, and transactions across a variety of product lines and systems, including deposits, wires, loans, trust, brokerage, letters of credit and check imaging applications. Each institution will have to identify the vendor that best meets its needs.

Which automated tool is right for your organisation?

Each case will be different, depending on customer base, size and services offered. In general, however, if your organisation decides to buy software, look for these functional components:

- Ability to monitor transactions and identify anomalies that might indicate suspicious activity.
- Ability to gather CDD information for new and existing customers.
- Ability to conduct advanced evaluation and analysis of suspicious/unusual transactions identified by the monitoring system in the context of each client's risk profile and that of their peer group.
- Ability to view individual alerts within the broader context of the client's total activity at the institution.
- Workflow features, including the ability to create a case from an alert or series of alerts, and collaboration (simultaneous or serial) among multiple interested parties to view and update information, and the ability to share AML-related information across monitoring and investigating units.
- Ability to store and recall at least 12 months' data for trend analysis.

- Ability to manage the assignment, routing, approval and ongoing monitoring of suspicious activity investigations.
- Automated preparation and filing of STRs to the financial intelligence unit.
- Standard and ad-hoc reporting on the nature and volume of suspicious activity investigations and investigator productivity for management and other audiences.
- Ability to provide comprehensive and accurate reporting of all aspects of AML compliance, including reporting to management, reporting to regulators, productivity reporting and ad-hoc reporting.

In addition to these functionalities, evaluate the following aspects:

- Ease of use of the application, as well as the configuration of new and changed transaction monitoring rules.
- Ease of data integration, system implementation and configuration.
- Scalability of application – the ability of the system to grow with the institution.
- Price, including initial cost, ongoing costs to sustain the system or to expand the capabilities of the system.

Some popular tools/software are available which need to be evaluated based on the nature, size and complexity of transactions.

The above policies, procedures, systems and controls are not put in place and at times for business considerations these are not followed. As a result, year on year, RBI has imposed heavy penalties on Banks and it is continuing. ■