Compliance with AML & CFT Guidelines: A Review of Implementation in Banks

B. Viritha*, Dr. V. Mariappan**

Money laundering has negative consequences on country's economy, macroeconomic performance and social well-being. It is a threat to the integrity of financial institutions and exposes them to various risks like reputational, legal and integrity risks. An attempt is made in this paper to look at the current scenario of implementing anti-money laundering (AML) and combating the financing of terrorism (CFT) guidelines by the financial firms, in particular banks and identifies the factors for the failure of AML regime. Accordingly, the paper proposes for stronger regulatory framework for effective implementation of guidelines, up gradation in skill and improved attitudes of bank staff, better usage of technology in monitoring and identifying the suspicious transactions, better coordination and support from the regulators and intelligence authorities.

Keywords: Know Your Customer, Money Laundering, Terrorism Financing, Customer Due

Introduction

In the recent times, banks have been used by criminal elements for money laundering and terrorist financing activities which on one side pose a great threat to national and international security and on the other hand, creates a great loss to the Government exchequer. Thereby the regulators are attaching considerable importance to improve the ability to identify, measure, monitor and control money laundering risk.

Money laundering is the act of converting the money obtained by illicit activities to disassociate the real source of proceeds and making it to sufficiently appear as originated from a legitimate source. In simple words, it is the process of converting the black money to white money through sequential stages, namely placement, layering and integration. Contrast to money laundering where launderer attempts to delink the source of bad funds, terrorist financing is funding either the clean or the laundered money to terrorist organizations to help them to carry out terrorist acts.

It is also referred as 'Reverse Money Laundering', because the money is financed to commit crimes in future. Investigations of 9/11 attacks (Austrac, 2008; Raghavan and Balasubramaniyan, 2012)made it very clear that the financial facilitators of terrorist organizations played a vital role in transferring money through a series of bank accounts held in United Arab Emirates to US banks. A set of 24 US bank accounts were opened by 9/11 terrorists using false identities, social security number and other documents. Thus theft of personal identity information is a common method used by the criminals to gain access to the banking services. They moved money about US$325,000 from benefactor's accounts in Middle East to US banks through wire transfers, and used debit cards issued by foreign banks in US for accessing overseas accounts.

The globalization of national economies widened the scope for money laundering and terrorist financing.When one country strengthens its regulations and other countries remain without adequate regulations, money launderers and terrorists may transfer their criminal proceeds to countries where comparatively looser regulations exist (Kishima, 2004).Or vice versa can also happen where money placed in a bank branch in a less regulated jurisdiction is easily transferred internally within the bank to a branch in a more regulated jurisdiction. Generally banks, insurance companies, security markets, and other non-banking finance companies are the most favored channels of laundromats. Consequently the governments of various states reacted to these threats with the legislations on the Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) law and 'Know Your Customer' (KYC) by adding the obligation to banks to report all transactions that are potentially linked to terrorist financing (Naylor, 2007). Hence, financial institutions have to implement a strong customer due diligence (CDD) to disrupt Money Laundering, Terrorism Financing, and other related crimes, at the point of establishing a customer relationship and on an on-going basis thereafter. Know Your Customer (KYC) is the preliminary and essential feature of this due diligence that identifies the customer through valid identification documents.

AML compliance mandates banks to know their customers well, maintain adequate records, identify suspicious transactions and file suspicious transaction reports (STRs), follow well regulated internal audit mechanisms and have comprehensive programs for the training of staff. Having

*Corresponding Author, Research Scholar, Department of Banking Technology, School of Management, Pondicherry University
**Associate Professor, Department of Banking Technology, School of Management, Pondicherry, University

these measures in place is, however, only a first step towards establishing an AML/ CFT regime. Itis far more challenging to understand the extent of compliance and ensure their effectiveness. Recently a British based Multinational Bank was fined of $1.9 billion by US Justice Department for "stunning failures of oversight—and worse—that led the bank to permit narcotics traffickers and others to launder hundreds of millions of dollars through the Bank subsidiaries, and to facilitate hundreds of millions more in transactions with sanctioned countries." This calls for a closer inquiry of the AML practices and this paper presents the current scenario of AML/CFT implementation through the reviews that surveyed the AML/CFT regime between 2003 and 2012.

International and Regulatory Guidelines

The Financial Action Task Force (FATF) has set guide lines to effectively counter money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction, which are threatening the integrity of the international financial system. It has put forth forty recommendations on anti-money laundering and nine special recommendations on combating the financing of terrorism. These guidelines are revisited by the FATF, integrating most measures previously focused on terrorist financing throughout the recommendations, therefore obviating the need for the Special Recommendations (FATF, 2012). These guide lines are recognized as the global anti-money laundering and counter-terrorist financing and financing of proliferation standards. Today more than 180 countries have endorsed the FATF guidelines, though they vary in the level of enforcing these guidelines.

The Basel Committee on Banking Supervision (BCBS) strongly recommended the adoption of these FATF guidelines. It also opined that KYC procedures go beyond simple account opening and maintenance of records and required banks to effectively use the KYC safeguards in managing their risks. The committee requires banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities. Thus, Basel framed a four-pronged approach to KYC namely customer acceptance policy, customer identification, ongoing monitoring of accounts and transactions, and risk management (BCBS, 2001).

In India, a strong legislative support through enforcement of Prevention of Money Laundering Act (PMLA), 2002 for combating money laundering, Unlawful Activities (Prevention) Act, 1967 to combat terrorism and its financing, and Reserve Bank of India (RBI)'s KYC/AML/CFT guidelines and circulars issued to Scheduled Commercial Banks, Regional Rural Banks and Co-operative banks helps to curtail money laundering and terrorism financing. The RBI has adopted the FATF guidelines and Basel's approach to customer due diligence and issued the "Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002"toall the banking firms in India, with indicative suggestions wherever considered necessary. The Indian Banks' Association (IBA) had also issued guidance notes for banks on KYC norms and AML standards (IBA, 2009).

FATF recommended to adopt the home country regulations for the overseas banks and its subsidiaries (FATF, 2012), whereas Basel directed the banks to comply with laws and regulatory requirements of the host jurisdiction, as part of compliance (BCBS, 2005). RBI has adopted the stringent of the two in implementing KYC (RBI,2012). Thus the financial institutions in India have been bench marking their policies and procedures with global best practices because of their branches and subsidiaries in multiple geographies.

Customer Due Diligence (CDD) in Banks

The objective of CDD is to weed out the bad customers from using the financial institutions as a conduit for money laundering, terrorism financing and proliferation activities. This is facilitated through customer identification, transaction monitoring, and reporting, supplemented with software solutions, auditing and training. Without effective CDD measures, banks can become victims to reputational, legal and integrity risks and can also result insignificant financial losses.

The decision whether a customer is accepted or rejected is the easiest and earliest point to avoid the risk of money laundering and terrorist financing. Thus world-wide KYC policies are becoming increasingly important. KYC is a part of due diligence that financial institutions and other regulated companies and professions must perform to identify their clients and ascertain relevant information before doing business with them. The KYC comprises activities (Tonbeller AG, 2010) such as capturing the information through questionnaires (application forms), screening against sanctions list and watch lists, collection and verification of identification and any other relevant documents as required, initial risk assessment, deciding to accept or reject the customer, assigning expiration date for the KYC documentation and on demand and periodical reassessment of risk. The following Figure – 1 shows the process of customer acceptance in banks.

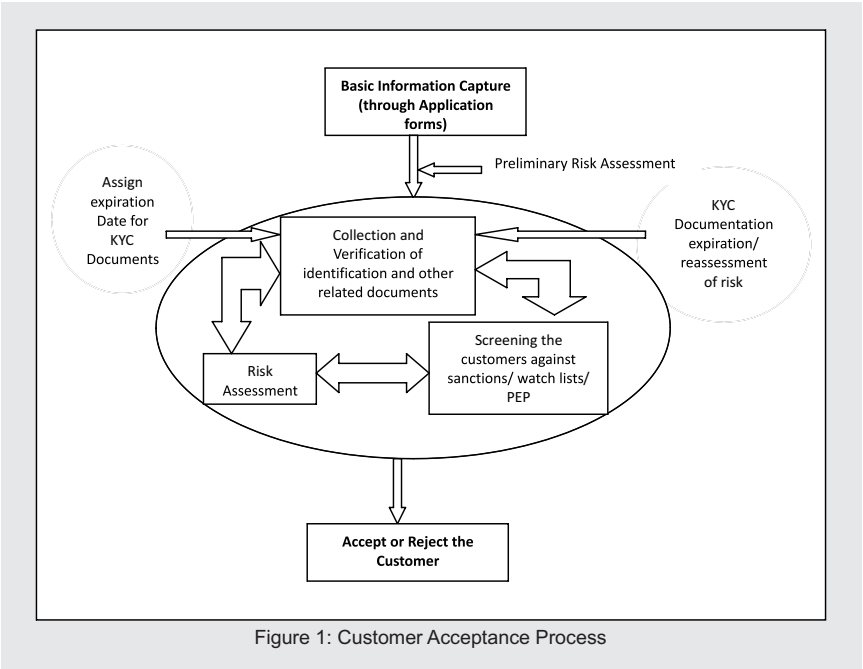

Figure 1: Customer Acceptance Process

When bank could not get the sufficient KYC information, the reasons for such non-availability of the required information have to be properly recorded and maintained. Additional information over and above identification information should also be obtained and used by banks to assess the risk of money laundering (FATF, 2012; BCBS 2001; Wolfsberg 2012). This will in turn facilitate monitoring, which is an essential anti-money laundering control. In Indian financial firms, thirteen percent of the respondents open accounts without fully collecting or verifying the documents (KPMG, 2012). While this might be a small percentage, it is worrisome because this is sufficient to meet the requirement of unscrupulous persons all over the world.

The identity of beneficial owners and politically exposed persons (PEPs) is difficult to establish, especially when dealing with overseas clients, and are found to be more vulnerable to the money laundering risk. The list of PEPs has to be extended to also include (Choo, 2008) individuals holding prominent public functions in their own jurisdictions; individuals exercising functions not normally considered prominent but having political exposure comparable to that of similar positions of prominence; and individuals holding important positions in private sectors such as CEOs of listed companies. Multi-jurisdictional corporate entities and trusts, specialized intermediaries and professionals, nominees and shell companies often hide the identity of the beneficial owner as well as the origin of the funds (Tonbeller AG, 2010).In such cases, it is vital to have experienced officers with good local contacts to pick up reliable information on the backgrounds of such potential clients through informal channels or specialist investigation agencies (FSA, 2007). However, the question of reliance on such information and the final decision to establish the relationship is left ambiguous.

Visiting the homes or business premises of high risk clients by the relationship managers (FSA, 2007), sending registered lettersto the given address of medium risk customers and retaining the signed return receipts (Tonbeller AG, 2010) should be made as a mandatory account opening requirement under the KYC process. Also, adoption of the Unique Identification Code by the banking system will help the banks in easy identification of the customer across multiple financial markets, track the facilities availed by them, and monitor financial transactions in various accounts in compliance with KYC/AML regulations. In the case of Indian context, Aadhaar card, being issued by the Government of India, is being leveraged upon by the banking system and must be sought as a document from the customer during customer identification thereby prohibiting the customers from circumventing the risk profiling guidelines and obtain multiple facilities across banks by opening several accounts (Chakrabarty, 2012; KPMG, 2012).

Risk Based Approach (RBA) to Customer Due Diligence (CDD)

In view of the voluminous work being handled by the banks, it is not possible to apply enhanced diligence for all the accounts and this is where risk based approach helps. The objective of risk based approach is to identify, assess, mitigate and monitor the money laundering and terrorist financing risks on a considered and continuing basis. The banks should continuously assess their risks for understanding the threats emanating from environmental factors such as regulatory or political changes, new developments in business where funds might be laundered or used for terrorism (Choo, 2008).

RBA is not only convenient for carrying out bank' sown activities, but also reduces the burden of low risk customers

(FSA, 2003).The first possibility of applying RBA in evaluating a customer is during the customer acceptance phase. RBA classifies the customers into low, medium, and high risk or any other risk ratingscaleas suggested by the bank policies, based on the risk factors identified from the 'customer acceptance matrix' (wit, 2007)which is a combination of customers and products/ services, with a consideration to the topologies published by the peer institutions. Thus, risk matrix forms the basis for assessing several risk indicators denoting that risk assessment is not one-dimensional and it considers products and services availed by the customers for evaluating the customer risk. Simonova (2011) opines that if product requested by a foreign PEP is deemed to be low risk, it is justified to apply simplified diligence on such customers. However, the low risk instruments such as a savings account too can prove risky given the ease with which it can be opened and operated. Thus it is always good to have a high diligence approach on high risk clients in spite of availing services with low risk instruments. An example of a risk matrix which may be used in relation to banking services is provided (see annexure). In Indian financial firms, the nature of the customer's business and background is given greater consideration when following a risk based assessment (KPMG, 2012).

During the transaction monitoring phase, the risk profile of the customer will help in understanding the normal activity of the account, which in turn will facilitate to identify any unusual activity(activity that deviates from the normal activity). It becomes easier for banks to monitor, when they could segregate the clients, especially high risk clients, further into different categories, based on the type of risk perceived from them. One UK firm (FSA, 2007) classified its high risk clients based on – clients having active financial links with countries included in the bank's 'hot-list'; clients engaged in 'tax aggressive' schemes; clients engaged in the sale or manufacturing business of armaments; clients engaged in businesses involving dangerous, radioactive or toxic substances and significant human or environmental risk; accounts with insufficient information about customer activities; accounts with suspicious activity report; account srequiring transaction level monitoring as considered by account officers.

Transaction Monitoring

The fundamental step in transaction monitoring is identifying the deviations from the normal or expected activity. These deviations constitute the unusual behavior of the client account. The unusual behavior is identified by comparing the account activity to its past behavior, and when it exceeds the set threshold levels. The account activity can also be analyzed in comparison to the account behavior of its client peer groups (Young, 2004).All unusual transactions may not be suspicious transactions (FSA, 2003), however vice versa is true. This unusual or suspicion can also be aroused through customer contacts (meetings, discussions, in-country visits etc.), third party information (e.g. newspapers, internet, vendor databases), and by utilizing relationship manager's corporate knowledge on customer's environment (FSA, 2007).

The activity of the account can be monitored either manually or it can be automated using technology with minimal and essential interference from the bank employee. Manual monitoring of transaction is labor intensive, in other words too costly (wit, 2007).The periodicity for manually reviewing the transaction activity of high risk clients was on a monthly basis, using a rolling three months of previous transaction data, whereas for medium risk, it was reviewed on a three monthly basis, using six months of transaction data and for low risk as and when deemed necessary(FSA, 2007).Thereby, considering cost and the ease of functioning, regulators are insisting for the use of software solutions for monitoring the transactions.

With regard to CFT, suspecting that a transaction is related to the financing of terrorism is more difficult than developing a suspicion that a transaction might be related to money laundering (Johnston and Carrington, 2006),sinceunderlying the terrorist transactions, there need not be any predicate offence, and the size of the transaction might not be inconsistent with the customer's regular activity. Hence the financial firms have to look into other indicators such as the recipient of the funds, or any other information that may create suspicion that a customer may be linked to the financing of terrorism. Financial intelligence is very essential in order to trace the roots of terrorism. The suspicious account linked to terrorist financing has to stay open, and operate so as to give the opportunity to the law enforcement authorities for monitoring and conducting their inquiries (Simser, 2011).Mere closing down the operations of such accounts will not shatter the objectives of the terrorists and they look forward to other means of transferring the money like bulk cash smuggling. Thus the legal framework has to provide provisions to enable banks to keep open and monitor such unscrupulous accounts.

Reporting and Feedback

Banks are exposed to legal risk on failing to meet reporting obligations. However, reporting for the sake of reporting or sending the reports just to avoid any mistakes and under reporting (Subbotina, 2009) on part of banks would not serve the purpose and does not satisfy the bank's obligation to contribute meaningfully to a sound and effective national AML/CFT regime. Defensive reporting burdens the FIU with overwhelming information and thereby reducing the resources available to investigate reports that merit further enquiry(Johnston and Carrington, 2006). Thus the quality of the information reported is very essential for taking the investigations on right track. The number of qualitative STRs reported ensures the effectiveness of AML/CFT regime. At least initially, decrease in the number of STRs does not indicate an improvement in AML/CFT regime, despite of strong KYC practices in place. It means that it has created a significant impact on the money launderers from using the financial system. So, the STRs eventually should increase, until the

criminals and money launderers realize that they may be subject to disclosure reports if they approach a financial intermediary (Chaikin, 2009).

The PMLA 2002 has casted obligations on banking companies, financial institutions, and other intermediaries such as stock brokers, merchant bankers, underwriters, etc. in India for furnishing information on cash transactions of rupees ten lakhs and above or its equivalent in foreign currency, all series of cash transactions valued below rupees ten lakhs but integrally connected to each other within a month, suspicious transactions and counterfeit currency transactions (CCR) to the FIU – India. The trendon year on year basis in the number of CTR, STR and CCR reports received by the FIU- India from banks is shown in Figure 2. The Table 1 below provides the total number of reports submitted by the banking sector to the FIU-India.

Table 1: Volume of Transaction Reports Submitted by Banks

Financial Year	CTR	YoY Change (%)	STR	YoY Change (%)	CCR	YoY Change (%)	Total
2007-08	6,100,681	-	1,183	-	8,580	-	6,110,444
2008-09	5,511,150	-9.66	2,826	138.88	35,730	316.43	5,549,706
2009-10	6,694,404	21.47	7,394	161.64	127,781	257.63	6,829,579
2010-11	8,687,107	29.77	12,287	66.18	251,448	96.78	8,950,842
2011-12	10,198,262	17.40	14,949	21.67	327,382	30.20	10,540,593

Data source: FIU – India

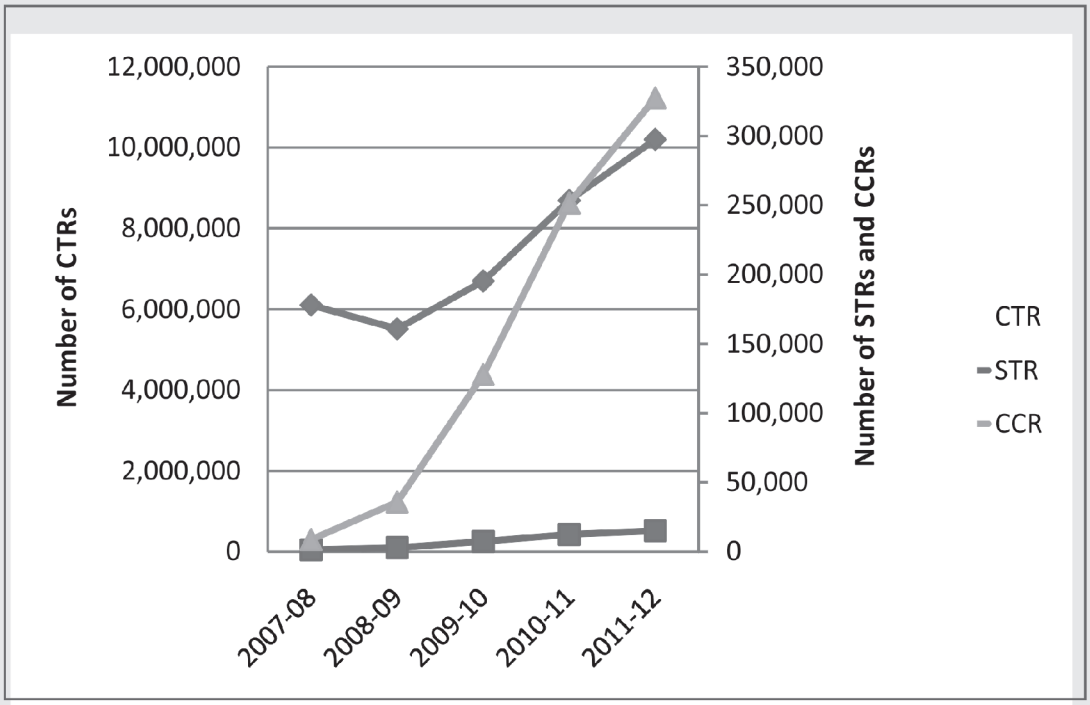

Figure 2: CTR, STR and CCR trend reported by Indian banks

It is evident that when compared from 2007 to 2012, CTRs, STRs and CCRs have experienced a growth of 67%, 1164% and 3716% respectively. This may be due to the stringent norms that have led to the increase in volume of reporting by banks. The growth trend is increasing but at a diminishing margin which indicates the prudence of norms being implemented over a period of time.

Auditing and Training

The KYC activities have to be subjected to periodic and independent review by the internal audit function (BCBS, 2005), by regulators and third party auditors, as auditing plays a key role in enhancing the compliance and quality through the KYC review process. Lack of audit function will hide the lapses if any that will make banks more vulnerable to the risks. Mostly, banks are assessed by the internal and external auditors and AML auditing by regulators is found less in banks. The commercial banks in China, between 2006 and 2010, were never been assessed by its regulator, for compliance with AML regulations (Simwayi and Guohua, 2011). Regulatory compliance and process effectiveness will be put to stake without AML auditing in place by regulators.

The training aims at providing the knowledge and skills required to implement the function and at least every two years the staff dealing with clients have to be trained on AML. The financial institutions in India are imparted with role specific training through face to face delivery training and computer based training methods by its internal trainers. The AML compliance is being used as a parameter to measure the performance of senior management to keep them accountable for their AML practices in the bank (KPMG, 2012).

Role of Compliance or Money Laundering Reporting Officers (MLRO)

An individual with greater competence is required in the exercise of compliance function and therefore the educational background, experience and attitudes (Webb, 2004; Verhage, 2009) form important elements of compliance officers for their effective functioning. The majority of the MLROs perceived regulations and practices are good only to the well-being of the community and world and there is no benefit to the bank, whereas only few were of opinion that these are good for both the bank and the society. Negative attitudes too existed where they felt that KYC did not have any effect in preventing money laundering since it is easy to obtain false identification papers if required(Webb, 2004).

MLROs are having other responsibilities apart from the AML compliance and this reduces the time spent on the compliance function. However, there is no correlation between the size of the bank and time spent by the MLRO on their AML duties as MLROs in the medium and large sized banks had other staff in their department to assist with the money laundering function. MLROs felt that KYC was the most time consuming part of the money laundering compliance subsequently followed by transaction monitoring. They perceived KYC rules were considered intrusive by many customers. They also felt that KYC should not be retrospective for long standing customers (KPMG, 2012).

Factors for Failure of AML Regime

The failure of AML regime is attributed to the various factors like lack of risk based approach to conducting KYC (Jun and Ai, 2009), flexibility of AML laws which are interpreted in different ways by the practitioners and lack of understanding of international or regulatory AML standards(Subbotina, 2009), lack of feedback from FIU and other regulatory bodies on the effectiveness of the measures taken by the banks (Webb, 2004; Subbotina, 2009; Verhage, 2009; Simser 2011). The failure of the regulation is also attributed to the lack of willingness of the staff participating in the compliance function. Subbotina (2009) noted that Russian banks failed since the AML activities were driven by fear of revocation of banking license, rather than desire to contribute to the fight against money laundering. Harvey and Lau (2009) also indicated that compliance was undertaken in order to avoid the impact of a fine, rather than to preserve the reputation of the financial sector and it was evident from the reports of the UK banks, where very little was disclosed about their money laundering compliance activity. When there is a link between anti-money laundering compliance and reputation, banks would consider disclosing its merits on compliance of AML for public to gain repute. In case of Belgian banks, the fear of reputational harm was a driving force for compliance, and it outweighed the other losses resulting from sanctions (Verhage, 2009). Though it is on a positive note, they yet lacked in truly serving the objectives of AML.

The attitudes of the senior management of commercial banks in China (Simwayi and Guohua, 2011) were positive in combating money laundering but the junior members of the staff perceived AML activities as an extra burden on the functioning of the banks. It is the responsibility of the regulators to understand the nature of the burden on part of the reporting entities, if resistance to the money laundering regime has to overcome and develop more positive attitude among the stakeholders of the AML regime (Webb, 2004). It is evident from the above studies that the effective implementation is a dependent function of the attitudes of staff.

Conclusion

A great deal of ambiguity and unwillingness exists in determining how to comply with the guideline requirements in achieving an effective compliance program. Adding to it, the guide line vagueness makes it difficult for the implementation of AML. So, a clearly documented AML policy and practices, customized to the type of banking operations should be made available by the senior management of the banks to implement the AML standards without any ambiguity. Also, Training materials and written communications should be tailored to

the employee role so that they can be understood by the target audience and thereby facilitate in their development of AML knowledge and skills. The technology has to be leveraged upon with efficient risk based models in place, to strengthen the monitoring system of the banks to identify the suspicious activities of the customer. The bank management should take the responsibility of nurturing the attitudes of their employees towards serving the society in curbing the menace of anti-social elements and become willing partners of the AML regime. To encourage the effective compliance program in banks, regulators should take the responsibility of providing incentives for banks that consistently comply to the standards effectively. The feedback and support system from regulators and intelligence authorities has to be well developed to facilitate the bank to be on the right track of implementation. Without feed back,i t is like a black box, where the outcomes are not known for the efforts taken. Hence, the developments in these elements will take the compliance to further heights.

References

Austrac. (2008, December 12). *Terrorism Financing.* Retrieved March 17, 2013, from Australian Transcation Reports and Analysis Centre: http://www.austrac.gov.au/elearning/pdf/intro_amlctf_terrorism_financing.pdf

Basel Committee on Banking Supervision. (2001). *Customer due diligence for banks.* Bank for International Settlements, Basel.

Basel Committee on Banking Supervision. (2005). *Compliance and the compliance function in Banks.* Bank for International Settlements, Basel.

Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control, 12* (3), 238 – 253.

Chakrabarty, K. C. (2012). Indian banking sector – towards the next orbit. *9th Advanced Management Programme* . International Management Institute, New Delhi.

Choo, K.-K. R. (2008). Politically exposed persons (PEPs): risks and mitigation. *Journal of Money Laundering Control, 11* (4), 371 – 387.

FATF. (2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.* Paris.

FIC. (n.d.). *General Guidance Note Concerning Identification of Clients.* Retrieved March 17, 2013, from Financial Intelligence Centre, Republic of South Africa:https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf

FSA. (2003). *Reducing money laundering risk: Know Your Customer and anti-money laundering monitoring.* London.

FSA. (2007). *Review of private banks' anti-money laundering systems and controls.* London.

Fleming, M. H. (2005). *UK Law Enforcement Agency Use and Management of Suspicious Activity Reports: Towards Determining the Value of the Regime.* University College London.

Harvey, J., & Lau, S. F. (2009). Crime-money, reputation and reporting. *Crime, Law and Social Change, 52*, 57-72.

IMF and World Bank. (2004). Financial Intelligence Units: An Overview.Washington, D.C.: International Monetary Fund.

Indian Banks' Accosiation. (2009). *Guidance notes for banks: Know Your Customer (KYC) Norms And Anti-Money Laundering (AML) Standards.* Mumbai.

Johnston, R. B., & Carrington, I. (2006). Protecting the financial system from abuse: Challenges to banks in implementing AML/CFT standards. *Journal of Money Laundering Control, 9* (1), 48 – 61.

Jun, T., & Ai, L. (2009). The international standards of customer due diligence and Chinese practice. *Journal of Money Laundering Control, 12* (4), 406 – 416.

Kishima, K. (2004). Japan's efforts in the global fight against money laundering and terrorist financing. *Journal of Money Laundering Control, 7* (3), 261 – 263.

KPMG. (2012). *India: Anti-Money Laundering Survey 2012.*

Naylor, R. (2007). Criminal Profits, Terror Dollars and Nonsense, Tax Justice NL. *Seminar on Money Laundering.* Amsterdam.

Raghavan, S., & Balasubramaniyan, V. (2012). Financial facilitators: an important component of terror networks. *Journal of Money Laundering Control, 15* (3), 294 – 303.

Reserve Bank of India. (2012, July 2). *Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002.* Retrieved July 5, 2012, from Reserve Bank of India: http://rbidocs.rbi.org.in/rdocs/notification/PDFs/34MCKY020712.pdf

Simonova, A. (2011). The risk-based approach to anti-money laundering: problems and solutions. *Journal of Money Laundering Control, 14* (4), 346 – 358.

Simser, J. (2011). Terrorism financing and the threat to financial institutions. *Journal of Money Laundering Control, 14* (4), 334 – 345.

Simwayi, M., & Guohua, W. (2011). The role of commercial

banks in combating money laundering. *Journal of Money Laundering Control, 14* (4), 324 – 333.

Subbotina, N. (2009). Challenges that Russian banks face implementing the AML regulations. *Journal of Money Laundering Control, 12* (1), 19 – 32.

Tonbeller AG. (2010). *Whitepaper: Keep Money Laundering and Fraud out - Know your Customer (KYC).*

Verhage, A. (2009). Compliance and AML in Belgium: a booming sector with growing pains. *Journal of Money Laundering Control, 12* (2), 113 – 133.

Webb, L. (2004). A survey of money laundering reporting officers and their attitudes towards money laundering regulations. *Journal of Money Laundering Control, 7* (4), 367 – 375.

Wit, J. d. (2007). A risk-based approach to AML: A controversy between financial institutions and regulators. *Journal of Financial Regulation and Compliance, 15* (2), 156 – 165.

Wolfsberg. (2012). *Wolfsberg AML Principles on Private Banking*. Retrieved from The Wolfsberg Group: http://www.wolfsberg-principles.com/privat-banking.html

Young, C. (2004). Periodic account activity and automated money laundering detection. *Journal of Money Laundering Control, 7* (4), 295 – 297.

Annexure

Risk Indicators Concerning Products

Risk Indicators Concerning Clients	Loan and credit	Mortgage bond no access	Mortgage bond access facility	Current <20K rolling average	Current 20–50K rolling average	Current 50–100K rolling average	Current >100K rolling average	Business 50–100K rolling average	Business >100K rolling average	Private banking	Niche product	Correspondent banking
SA citizen	10	10	20	10	20	30	40	30	40	50	50	50
SA institutional client	10	10	10	10	10	20	20	20	30	-	50	50
SA listed company	10	10	10	10	10	20	20	20	30	-	50	50
Wholly owned subsidiary of SA listed company	10	10	10	10	10	20	20	20	30	-	50	50
SA (Pty) Ltd's& CC's	10	10	20	10	20	30	30	30	40	-	50	50
SA PEP	20	20	30	20	30	40	40	40	50	50	50	50
SA trust, partnership & other	20	20	30	20	30	40	50	40	50	-	50	50
Foreign national: A country	20	20	30	20	30	40	50	40	50	50	50	50
Foreign listed company: A country	20	20	20	20	30	40	20	40	40	-	50	50
Foreign institutional client: A country	10	10	20	20	20	30	20	30	30	-	50	50
Foreign national: B country	30	30	40	30	30	40	50	40	50	50	50	50
Foreign institutional client: B country	20	20	30	10	20	30	30	30	30	-	50	50
Foreign listed company: B country	20	20	30	20	30	30	30	40	40	-	50	50
Foreign company: A country	20	20	30	20	30	40	40	40	50	-	50	50
Foreign company: B country	20	20	30	30	30	40	50	40	50	-	50	50
Foreign trust, partnership & other	50	50	50	50	50	50	50	50	50	-	50	50
Foreign client: C country	50	50	50	50	50	50	50	50	50	50	50	50
Foreign PEP	50	50	50	50	50	50	50	50	50	50	50	50

Additional weighting based on client attributes:	Client on UN List	+50	
	< 1 year relationship	+30	
	1 – 5 year relationship	+15	
	Financial institution / intermediary acting obo client	+10	
Additional weighting based on nature of product:	Credit with term < 6 months	+30	
	Credit with term 6 months – 1year	+10	
	Facilitates cross-border movement of funds	+20	
Additional weighting based on source of funds:	Dealer in high value goods	+30	
	Import / export	+30	
	High cash generating	+30	
Additional weighting based on client conduct:	Client's prospective use lack business sense		+40
	Unusual concern for secrecy		+40
	Refuses / fails to indicate / vague as to source of funds / nature of business		+40
	Lack of concern for high risk / transaction costs etc		+40
	Lack of general knowledge re industry		+30
Country classification:	A:	Members of FATF, except USA and UK	
	B:	Non-Members of FATF + USA and UK	
	C:	NCCT listed	
Risk classes:	10 – 29:	Low	
	30 – 39:	Medium	
	40 and higher:	High	

Courtesy: Financial Intelligence Centre, Republic of South Africa