International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Anti-Money Laundering: Risk Management Framework

Anirudha Mishra
Master of Computer Application
ASM Institute of Management & Computer Studies
University Of Mumbai.
Mumbai, India

Abstract:

In this article, we propose strategies for AML where financial institutions can analyze, detect and report suspicious activity based on risk assessment. In order to support the AML Compliance risk management program, institutions must rely on data, multiple systems, and technology. Since the 2008 financial crisis link between internal audit, compliance, and risk management operations has been in light. One of our suggestions is to appoint a senior compliance officer, third-party internal audit, and give all the possible resources to the chief AML officer of the AML program. Training employees of financial institutions could be a boost.

Keywords:

Anti-Money Laundering, Compliance Program, Risk Assessment, CDD, FIU, Internal Audit.

I. Introduction:

Money laundering was uncovered in 1998 by the then-director of the International Monetary Fund (IMF), who believed it to be responsible for two to five percent of global GDP at the time. For instance, "Wachovia" (since merged with Wells Fargo) was hit with one of the highest fines for AML non-compliance at the time, in 2010. Drug gangs in Mexico are believed to have laundered upwards of $390 billion through the bank's branches. Due to Mexico's low AML rules, the bank did not conduct due diligence on the source of funds. As a result, criminal earnings have become part of the legal economy. Shell firms formed in the UK, for example, were linked to the laundering of £80 billion in stolen funds from 2010 to 2014.

Money laundering is the practise of presenting illicit wealth as genuine. According to the United Nations (UN) 2000 Convention [1], act or process of transferring an asset with awareness that it originates from an illicit source in order to conceal that source or help the offender involved in criminal activity. Its goal was to keep the nature and origin of illegally obtained cash hidden from tax officials and law enforcement agencies while integrating them into the economic institutions. Apart from unlawful operations like drug trafficking, cybercrime, and corruption, there are also quasi-legal businesses that hide money from government officials. The shadow economy evolves as a result of such actions. They also help in money laundering. The three stages of money laundering are placement, layering, and integration.

The Vienna Drug Convention, also known as the UN Convention on Narcotics and Other Psychoactive Substances, was the first global response to money laundering. If offenders are detected trying to launder money originated from the manufacture/sale of narcotics, they may be prosecuted under the accord. In 1989, the Group of Seven (G7) established the Financial Action Task Force (FATF) to address the rising problem. The FATF has broadened its definition of money laundering to include proceeds from other illicit actions such as illegal weapons sales, insider trading, embezzlement, bribery, and forgery. Since then, the definition of money laundering regulations has been broadened on a regular basis in an effort to combat this rising problem, such as to encompass activities that finance it. [2].

II. Literature Review

To comprehend a problem, you must first understand its scope. This allows for a long-term evaluation of the severity of the crime, its macroeconomic effects, and the effectiveness of countermeasures. When it comes to money laundering, the same is true. The amount of money laundered has been quantified by researchers. Walker's work is widely recognised in this subject [3][4]. The investigation unveiled the "Walker model of global money laundering," which is driven by a number of publicly accessible data sources. In 1999, the global sum of money susceptible to laundering was US$2.85 billion annually, according to the model, with the majority of transactions originating in Europe and North America.

Since then, lots of new research have concentrated on figuring out how much money is laundered and how it is laundered [5]-[14]. Researchers have employed case studies, proxy variables, and economic models. According to Unger [2], money laundering may be measured in two ways: first by GDP, global proceeds of crime, and balance of payments imbalances and second by using economic models such as dynamic two-sector model and Walker-Gravity model. Although, some argue that these data are incorrect and deceptive when it comes to calculating the correct amount of money being laundered. According to Unger, the absence of a clear approximation of the sum of money laundering is linked to the underlying crime's secrecy.

A. Regulations, laws, and standards:

The Financial Action Task Force (FATF) and it's 40 Guidelines are at the head of the global anti-money laundering (AML) regulatory structure, which is effectively a "top-down" cascade. FATF has a mandate to set international anti-money laundering standards, but it lacks legal capacity to enforce legislation as a purely intergovernmental organisation. The FATF's members are accountable for maintaining that their policies, statutes, and institutions satisfy the group's basic standards. FATF's growing duties include assessing country implementation of recommendations, acts as a mentor on sectoral or financial criminal offences, and suggesting future adjustments to meet changing requirements.

The 40 Recommendations have maintained two fundamental features throughout their evolution:

- In Prevention: The three essential tasks for obligated institutions are Customer Due Diligence (CDD), reporting suspicious transactions to a national Financial Intelligence Unit (FIU), and retaining information for possible future use by investigators. The above is supervised by a regulator.
- In Enforcement: The processing and distribution of STRs to law enforcement and prosecuting authorities is the responsibility of FIUs. Information from the obliged sector is used to enhance investigations, prosecutions, and asset recovery. FIUs also sustain international interaction in cross-border circumstances.

Some organizations, mostly slim and emerging organisations, have been able to preserve their unique monitoring approaches while adhering to the FATF guidelines and norms and regulations that follow it under Risk Based Approach. Nonetheless, most financial institutions have embraced a uniform structure focused on automated rules-based platforms, high-volume alert triage, and inquiry throughout the industry. It was normal for an automated platform to be constructed in-house within the first decade of the surveillance requirements, often utilizing pre-existing credit risk and fraud models. Standard models from prominent technology suppliers are increasingly being purchased by financial organisations.

B. Anti-money laundering risk assessment

Anti-Money Laundering risk evaluation techniques are created by AML teams and inspection teams and are a critical component of developing a program which can locate, evaluate, and report suspicious behaviour within accounts [15]. Since the 1970s, when the Bank Secrecy Act was enacted in an attempt to restrict the threat of narcotics reaching the US market, the risk of money laundering really hasn't dropped. Instead, thanks to technological advancements and the increased speed with which money can be transmitted over the world, ML schemes have become increasingly sophisticated. As a result of the increase in money laundering, financial organizations are under immense pressure to spend more in anti-money laundering (AML) evaluation methods, or risk hefty regulatory fines. As per KPMG's 2014 [16] Global Anti-Money Laundering Survey, financial institutions have shown lack of investment in AML compliance in recent years. According to KPMG, some of these expenses may be due to regulatory agencies' demands for sudden change, which could explain why, provided the regulatory focus on transaction reporting, so a lot of the existing and proposed investment is being guided toward improving transaction monitoring and KYC programs.

As per the findings of the KPMG investigation, many AML strategies are being designed in reaction to regulatory demands vs being purposely engineered by the institutions themselves. Banks now must assess if it is more effective to harvest local intel and create their own risk-based program, or perhaps to rely for intellect that has been validated by regulators to determine where AML investigations must be focused. This might be a system based on the local money laundering patterns that only needs to be upgraded when international restrictions change, rendering it less unpredictable and easier to budget for.

Over the years, risk measuring, monitoring, and reporting, as well as the technology that supports these procedures, have changed. Institutions must now depend on information, different systems, and tools to facilitate their AML compliance programme. The quantity of technology employed will be influenced by the magnitude and sophistication of the institution. The principal AML officer ought to have exposure to and benefit from the IT system, even if it is administered or used by other lines of business, to the extent that it is important to his or her work.

III. Anti-money laundering investigation teams

When it gets down to detecting vulnerabilities and reviewing internal suspicious alerts, AML investigations demand a collective approach. Software can help with AML detection, but only if it is trained to check for suspicious transactions. The user is most important asset in an AML software. He/she is the one who program the software to look for suspicious transaction, also at the same time operator is competent to understand and act upon the data received from software. Human investigation has been at the heart of detecting frauds and AML infractions, and training is an area which is well worth investing in. Despite the fact that financial institutions employees are not members of law enforcement agency, the distinction between these two are becoming increasingly thin.

The significance of an institution's system of internal control to the organization's safe and secure operations, along with its risk management system, is widely known. Perhaps one of the major roles of senior management is to design and maintain an effective system of controls, which includes adequate role division and formal reporting system.

The relationship between internal review, compliance, and risk management processes has come under heightened regulatory scrutiny since the financial meltdown of 2008 [17]. Internal audit's role in complementing a broader risk management system and monitoring business line management, risk management, compliance, as well as other control functions has aroused regulators' interest around the world. Regulators want an institution's risk management function to be successful, as well as a compliance unit and an internal audit unit..

When it comes to AML risk management, the front end client facing business units are all still in charge of detecting, evaluating, and managing risks in their specific business sectors. (Because AML requirements and standards are always evolving, it is common for other divisions to give technical support as well as conduct the AML risk assessment.)

An AML officer may undertake some responsibilities in today's environment, such as monitoring for suspicious activity, initial and continuing customer onboarding screenings, and sanctions compliance screenings, in addition to conducting compliance testing that can be accessed by internal audit. The unit should be informed of and follow the guidelines and regulations, as well as be provided with adequate resources. Internal audit has similar responsibilities and roles, but it also supervises this highly specialized and risk-based compliance domain

A. Operational Management Unit

The operational management unit is responsible for finding, evaluating, limiting, managing, and reporting upon risks encountered across an institution's commercial activities. This unit is also the business generator. It is responsible for creating and adhering to risk-taking boundaries, policy guidelines, and the implementation and use of approved procedures. At the highest levels, it is also critical in setting an institution's risk-taking limitations. Through a cascading responsibility structure, managers typically formulate and maintain specific systems that act as checks and monitor their employees' implementation of such procedures.

By engaging with consumers, managing relationships with customers, and adhering to established policies and procedures, employees in the unit play a vital role in AML risk management. This unit is vital for identifying anomalous and suspicious activity, which is one of the most important AML reporting duties. Employees may notice odd or potentially suspicious conduct and/or behaviour by consumers throughout their daily duties. According to regulations and procedures, these personnel must be alert in identifying, escalating, and reporting potentially suspicious and perhaps anomalous behaviours. Management should ensure that every employee, specifically those who have direct interaction with customers, execute the internal procedures for detecting and reporting potentially suspect activity.

The institution's approach to potential vulnerabilities, including methods for dumping the client, contacts with intermediaries, as well as internal assessments of previous consumer behaviours, must be apparent to management. An organisation must have suitable rules and processes in place for screening potential and present people to make sure that highest professional and ethical standards are followed. AML compliance can be seen as a shared effort inside the institution.

The importance of staff training cannot be overstated. The scope and timing of such training should be adapted to the possible causes to which individuals are exposed as a result of their jobs, as well as the amount and kind of risk in the institution. All institutions should have continuous employee training programmes in place to ensure that their employees are properly taught to carry out the institution's policies and procedures. The institution will need to tailor the time and content of training for diverse sectors of staff based on their needs and the institution's risk profile. Depending on the duties and responsibilities of the personnel, several types of training will be required.

Training courses and resources should be customized to the individual's unique job or role to guarantee that an employee has adequate information and awareness to successfully integrate the institution's AML policies and procedures. For the same reasons, new employees should be persuaded to undergo training as quickly as possible. Employees should be given refresher training to remind them of their obligations and to maintain their skills and experience current.

B. Risk Management, Compliance, And Other Monitoring Units

These are control unit's that guarantee risk-related policies and procedures (risk management, compliance risk, hr, and legal) are in place and followed. The risk management team supports and supervises the implementation of effective risk management techniques by business-line management. It helps business line management to identify and report risk exposures across the company. The compliance function monitors the risk of disobedience with laws, regulations, & standards. Two distinct monitoring functions are human resources and the legal department.

In most institutions, the chief AML officer is responsible for the continuing completion of all AML duties by the institution. Based on the scale and sophistication of the institution, the chief AML officer may also be known as the Chief Risk Officer (CRO), Chief Compliance Officer (CCO), or something similar. He or she should be able to speak directly with the board of directors or a board-appointed committee.

Suspicious transactions should be reported to top leadership, the board, and the relevant Financial Intelligence Unit (FIU) by a AML executive. The institution's chief AML executive should be given the resources he or she needs to properly complete all of his or her responsibilities and to perform a prominent and active part in the institution's AML programme. To do so, he or she must be familiar with the institution's anti-money laundering (AML) programme, and also the institution's legislative and regulatory requirements, applicable international standards, and ML/FT risks.

C. Internal Audit Unit

The internal audit unit is tasked for objectively analysing the effectiveness of internal controls and compliance practises to rules, and regulations. On an annual basis, internal audit delivers a full review of their inspection procedures and relevant legal compliance. External auditors can play a critical part in evaluating an institution's internal processes and controls during audits, internal control audits, and anti-money laundering audits. External auditors can independently confirm an institution's adherence to local rules, supervisory methods, and correspondent financial institution expectations.

Internal audit plays a key role in the oversight framework by autonomously and objectively assessing risk management and controls and reporting just on efficacy of compliance with AML policies and procedures to the board or a board-appointed committee (such as an audit committee or a similar oversight body) on a regular basis. An institution's internal audit programme should include everything. For instance, the strengths of compliance management and supervision, the relevance of both the institution's policies and practices in attempting to resolve identified risks (which include AML), the expertise of institution staff in following this process and risk mitigation, the extensive testing of important internal systems, like suspicious activity monitoring as well as investigations processes, as well as the effectiveness of the institution's employee training.

To carry out such audits, the board needs practically ensure that the audit functions have adequate resources, expertise, and understanding of the institution's activities. The board should also ensure that the audit strategy and methodology, and the regularity of such audits and testing, are suitable for such institution's risk profile. Finally, internal auditors should preserve a paper trail of their findings and recommendations so that they can submit them to a board committee having responsibility of the internal audit process and business lines.

IV. Conclusion

The Strong Anti-Money Laundering Compliance Program should prioritise the institution's internal controls and processes for reporting and detecting financial crime. Internal controls include features like proper authorization, legal documentation, reconciliation, security, and role separation, to name a few. The programme should include a regular evaluation to ensure the effectiveness of these controls. The company's actions should be guided by defined policies and procedures.

The institution shall comply with all registration, transaction activity documentation, client identification verification, record retention, currency transaction reporting, monetary instrument tracking, suspicious activity reporting, and other obligations. In order to dissuade criminals from funnelling their illegal funds into the banking system, thus enforcing Prevention of Money Laundering Act 2012[18].

An effective Anti-Money Laundering Program should assign a senior compliance officer to oversee the general application of AML legislation throughout the institution. Employees who may get involved in a money laundering scheme, either directly or indirectly, are monitored by a complaint officer.

Communication with regulators and auditors, informing top management, and recommending AML policies based on audits and reports are just a few of the duties. While task completion is proportionate to the risks faced by the company.

As we all know, any Money Laundering Compliance Program can be vulnerable, so expanding the scope of AML programmes might be beneficial. Employee engagement in the AML programme must therefore be made mandatory. Employees can increase their knowledge and skills through a variety of institutions' training programmes. A successful training programme will not be "one size fits all," but rather tailored to the needs of the individual. As a result, we may argue that it will always have a loophole that the corporation must monitor.

As a result, we recommend that the institution's financial accounts be audited by a third-party company. Independent audits should be undertaken once a year, with institutions in high-risk areas being examined more frequently. The audit's purpose is to see if the software is functioning properly and if internal controls are in place.

References

[1]. UNODC (2004), "*United nations convention against transnational organized crime and the protocols thereto*", Vienna.

[2]. Unger, B. (2013), "*Can money laundering decrease?*", Public Finance Review, Vol. 41 No. 5, pp. 658-676.

[3]. Walker, J. (1999), "*How big is global money laundering?*", Journal of Money Laundering Control, Vol. 3 No. 1, pp. 25-37.

[4]. Quirk, P. (1997), "*Macroeconomic implications of money laundering*", Trends in Organized Crime, Vol. 2 No. 3, pp. 10-14.

[5]. Ardizzi, G., Petraglia, C., Piacenza, M., Schneider, F. and Turati, G. (2014), "*Money laundering as a crime in the financial sector: a new approach to quantitative*

assessment, with an application to Italy", Journal of Money, Credit and Banking, Vol. 46 No. 8, pp. 1555-1590.

[6]. Argentiero, A., Bagella, M. and Busato, F. (2008), "*Money laundering in a two-sector model: using theory for measurement*", European Journal of Law and Economics, Vol. 26 No. 3, pp. 341-359.

[7]. Barone, R. and Masciandaro, D. (2011), "*Organized crime, money laundering and legal economy: theory and simulations*", European Journal of Law and Economics, Vol. 32 No. 1, pp. 115-142.

[8]. Barone, R. and Schneider, F.G. (2018), "*Shedding light on money laundering. Is it a damping wave?*", SSRN Electronic Journal.

[9]. Hassan, M. and Schneider, F. (2016a), "*Modelling the Egyptian shadow economy: a MIMIC model and a currency demand approach*", Journal of Economics and Political Economy, Vol. 3 No. 2, pp. 309-339.

[10]. Hassan, M. and Schneider, F. (2016b), "*Size and development of the shadow economies of 157 worldwide countries: updated and new measures from 1999 to 2013*", Journal of Global Economics, Vol. 4 No. 3.

[11]. Medina, L. and Schneider, F. (2018), *Shadow Economies around the World*, in Schneider, F. (Ed.), International Monetary Fund, Washington, DC.

[12]. Schneider, F. and Enste, D.H. (2000), "*Shadow economies: size, causes, and consequences*", Journal of Economic Literature, Vol. 38 No. 1, pp. 77-114.

[13]. Unger, B. and Hertog, J. (2012), "*Water always finds its way: identifying new forms of money laundering*", Crime, Law and Social Change, Vol. 57 No. 3, pp. 287-304.

[14]. Walker, J. and Unger, B. (2009), "*Measuring global money laundering*", Review of Law and Economics, Vol. 5 No. 2, pp. 821-853.

[15]. Cindori, S. (2013), "*Money laundering: correlation between risk assessment and suspicious transactions*", Financial Theory and Practice, Vol. 37 No. 2, pp. 181-206

[16]. KPMG (2014), "*Global anti-money laundering survey*", available at: at: *www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3. Pdf*

[17]. Financial crisis of 2007-2008 *https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008*

[18]. Prevention of Money Laundering Act 2012. available at: https://dor.gov.in/preventionofmoneylaundering/str-suspicious-transaction-reports