Risk-based approach for designing enterprise-wide AML information system solution

Lishan Ai
*Centre for Transnational Crime Prevention, Faculty of Law,
University of Wollongong, Wollongong, Australia, and*

Jun Tang
*School of Information, Zhongnan University of Economics and Law,
Wuhan, People's Republic of China and
China Centre for Anti-Money Laundering Studies, Fudan University,
Shanghai, People's Republic of China*

Abstract

Purpose – This paper attempts to explain the key elements and associated definitions of the financial institutions' enterprise-wide anti-money laundering (AML) information system, and to discuss the technical theory for implementing the information system.

Design/methodology/approach – The paper defines the problems of defensive filing in the suspicious transaction reports, proposes AML practice from objective standard principle to subjective assessment principle, and provides detailed description of enterprise-wide AML solution.

Findings – As rule-based AML approach and objective-standard monitoring principle have led to numbers of practical problems, a significant tendency of regulatory reform is to replace the objective-standard principle by comprehensive risk-assessment process with considerations of the enterprise's reality.

Originality/value – The paper presents the latest development in enterprise-wide AML information system construction, including customer risk evaluation, transaction risk measurement, behavior monitoring technology, link analysis, risk ranking and workflow tools, etc. and major fundamentals and functions of these modules are also discussed.

Keywords Risk analysis, Enterprise-wide solution, Information systems, China, Financial institutions

Paper type Research paper

1. Introduction

Since 2003, the People's Bank of China has published anti-money laundering (AML)-related administrative rules that require financial institutions to implement the obligations of reporting large-value and suspicious transactions. With more efforts have been put into building up the Chinese AML mechanism, China has become a formal member of Financial Action Task Force (FATF) in August 2007. After this, Chinese authority has correspondingly enacted a series of AML legislations according to the international AML standards, including amendments of provisions on AML reporting by financial institutions, enhancement on customer identification program (CIP), and measures on combating terrorism-financing, etc. The challenges in current AML works for financial institutions are the massive number of suspicious transaction reports with limited information value, and the heavy working burden for data analysis and case investigation. In fact, the number of transaction reporting submitted

Journal of Financial Crime
Vol. 18 No. 3, 2011
pp. 268-276
© Emerald Group Publishing Limited
1359-0790
DOI 10.1108/13590791111147488

to the China AML Monitoring & Analysis Center (CAMLAC) has exceeded the sum of suspicious transaction reports from 16 AML-leading countries, including USA, UK, Japan, and Switzerland, etc. (Shi, 2007, p. 44). *The FATF First Mutual Evaluation on AML and Combating the Financing of Terrorism* in June 2007 clearly points out that the reporting system appears to operate principally as a rules-based unusual transactions regime. The majority of reported transactions can be reconciled quite simply with the customer's expected profile, but that reporting is still mandated (FATF, 2007, p. 93). The report further suggests that Chinese AML system should put significant concerns about the overall effectiveness of the system, and the lack of subjective assessment by reporting institutions is obvious (FATF, 2007, p. 97). Regarding on the research and development of AML information system solution, most of the previous works focused on how to utilize data-mining and business intelligence techniques to improve the deficiencies of the pre-established data-filtering system. Tang (2005) proposed to use the technique of behavior module detection in AML application, and Yang and Wang (2005) and Zhang *et al.* (2006) looked into the data-mining technique in money-laundering detection. However, all of these were topical studies, and the publication on integrated enterprise-wide AML information system which include data analysis sub-system and workflow sub-system is completely absent in this area in China. Based on the latest development on AML information system, this paper explains the key elements and associated definitions of the financial institutions' enterprise-wide AML information system, and discusses the technical theory for implementing the information system.

2. From objective standard principle to subjective assessment principle

2.1 Defensive filing in the suspicious transaction reports

Suspicious transaction report based on objective standards refers to a monitoring system utilizing pre-established indicators for money-laundering activities, and automatically giving a systematic alert when those indicators are detected. Following with the objective standard principle, regulatory departments does not have the real interest on the genuine value from the money-laundering risks in the suspicious transaction reports, but the reporting result *per se*. That is, when conducting regulatory examination, if financial institution is found out by the regulator that failed to make report which has unusual indicator, the financial institution will be imposed on monetary fine or administrative penalty. Owing to the financial institutions' staff universally lacked reporting awareness and detection capacity on suspicious money-laundering activities at the initial stage of Chinese AML practice, the traditional monitoring system with pre-established indicators was introduced to improve those two shortcomings at that time. However, the pre-established indicators are almost open to the public in forms of regulatory publications and AML legislations, which are possibly to be evaded from detection by the money launderers with intentions. Previous experiences showed that the inevitable consequence of the traditional monitoring system based on the objective standards is the prevailing of defensive filing. Faced by the penalty deterrence from regulatory authority, financial institutions act as their instinctive self-protections to choose the following reporting strategies – "making the report if the suspicious transaction is not assured", "reporting is better than non-reporting", and "the more reports the better" (Gao, 2007) – directly disobeying the original intention of effectively practicing AML mechanism.

2.2 Regulation reform from objective standard principle to subjective assessment
As rule-based AML approach and objective-standard monitoring principle have led to numbers of practical problems, a significant tendency of regulatory reform is to replace the objective-standard principle by comprehensive risk-assessment process with considerations of the enterprise's reality. Current AML legislations in the USA only set up the objective thresholds for large-value transaction reports. Instead of making any systematized financial transactional typologies or quantified determining criterion, the US AML authority hands the AML priorities of identifying, determining and dealing with suspicious transactions to individual financial institution. It requests the financial institution and its working staff to perform more pre-active in AML works with more sense of responsibility (Shi and Qiu, 2004, p. 11). With regard to improving the law enforcement process and dealing with defensive filing, Financial Crimes Enforcement Network (FinCEN) has worked with Federal Financial Institutions Examination Council (FFIEC, 2006, p. 56) for publishing and amending *The Bank Secrecy/AML Examination Manual* in consecutive three years since 2005. The BSA manual instructs that examiners should focus on evaluating a bank's policies, procedures, and processes to identify and analyze suspicious activity, rather than on a bank's decision with respect to any individual case. Thus, bank should not be criticized for the failure to file a suspicious transaction report unless the failure is significant or accompanied by evidence of intentionally bad faith. In addition, as the earliest country which applied suspicious transaction reports in 1986, UK has gradually encouraged financial institutions, in recent years, to take any measures to assist regulatory bodies tracing suspicious transaction activities with whole-hearted commitment (Kingdon, 2004, p. 87).

2.3 Principles for designing risk-based AML information system
To reflect the regulation reform from objective-standard principle to subjective-assessment principle on designing information system, is to change the traditional monitoring system with pre-established data-filtering project in the transaction database to the design of enterprise-wide AML risk-assessment process. The new system utilizes various risk-analysis tools to meet the requirements of risk-updating and risk-removing work, and scores the risk level based on the probability calculation. Risk analysis should impenetrate every business operations within the enterprise, including customer due diligence (CDD), and the amount, flow, frequency, business background, and associated individual or organizations of the transacted capital. From the perspective of analysis granularity, an accountable risk-level score can only be eventually made according to the comprehensive analysis on behavior pattern, which is constituted of individual and multiple transactions in the sequence of time, and the relationships among the transacted account, the transacted account holder, and the financial institutions of the transacted account holder. Apparently, designing the subjective-principle information system is much more complex than designing the pre-established data-filtering project. Via reforming the objective standard principle to risk-based approach, heavy burden of primary data analysis on the Financial Intelligence Unit (FIU)'s shoulder can be transfer to the customer's best knower: the financial institutions. In this way, the high-quality information can be layered and filtered from the massive reports by financial institutions, and then submitted to FIU for the follow-up analysis and investigation, achieving the practical effectiveness of AML monitoring system.

2.4 Enterprise-wide AML solution diagram

According to the above-mentioned principles, the information system can be divided into two parts: risk-analysis tools and compliance-supplementary workflow tools. Data-mining and business intelligence techniques are key components of risk-analysis tools, while any other factors for tuning the accuracy of risk assessment should also be integrated into the risk analysis. In particular, the risk-analysis tools contain due diligence system, transaction risk assessment, and comprehensive risk analysis. Workflow tools, on the other hand, are designed for legislatively-requested AML management works, for instance, data reporting and delivering, record keeping and searching, staff training, and case management. The flowchart of an enterprise-wide AML solution is shown at the end of this paper.

3. Description of enterprise-wide AML solution

An enterprise-wide AML information system solution comprises all kinds of money-laundering risk assessment systems, ranging from the front-client reception to the background analytics (Figure 1).

3.1 Customer due diligence

As the first step of risk-analysis process, customer reception in financial institutions is strictly examined by regulatory bodies, and it is the basic instrument to implement know your customer rules. *The Bank Secrecy Act/AML Examination Manual* published by FFIEC also emphasizes the meaning of CDD. FFIEC (2006, p. 56) states that:

> [. . .] the objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage, and these processes assist the bank in determining when transactions are potentially suspicious.

An effective AML compliance program includes due diligence around the account opening process that meets requirements identified in the CIP, including customer identity identification, and determinations on the actual beneficial owner and the actual account holder. Financial institutions should comply with the due diligence legislations to verifying the identification of the customer, and check the watch lists of high-risk customers if necessary. Based on determining the nature and purpose of transaction, the CDD system should be able to anticipate account activity according to the transacted amount, frequency of transaction, objectives of capital flow, and the geographic factor. Apart from the basic compliance requests in due diligence and account opening, this module should combine the enterprise's internal control, internal audit, and customer relationship management together.

3.2 Watch list

Watch list should be carefully checked both at the due diligence stage and link analysis stage. It is also an important reference of the case management module in the workflow tools. The watch list is periodically released by law enforcement agencies or related international organizations. The primary functions of this module are:

- allowing organizations to monitor all transactions involving certain individuals, relationships, products, organizations, or countries;
- identifying and generating automatic reports on particularly risky entities, such as non-cooperative countries (NCCT) list published by FATF, countries under

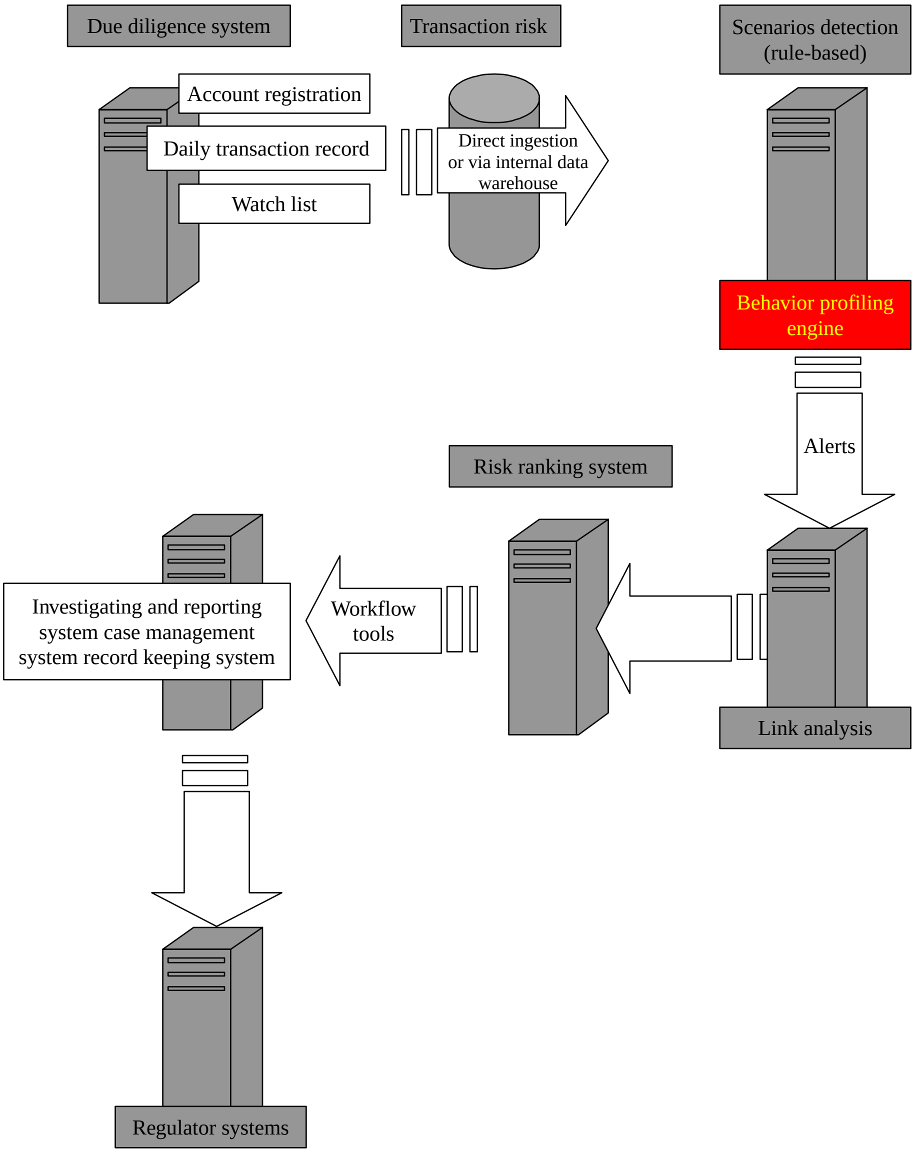
Due diligence system
Transaction risk
Scenarios detection (rule-based)
Account registration
Daily transaction record
Watch list
Direct ingestion or via internal data warehouse
Behavior profiling engine
Alerts
Risk ranking system
Investigating and reporting system case management system record keeping system
Workflow tools
Link analysis
Regulator systems

Figure 1.
An enterprise-wide AML solution diagram

international sanction, politically exposed persons, and high-risk transaction activities performed by particular individuals or organizations which are under investigation or penalties from law enforcement agencies; and

- establishing “zero risk” or “no problem absolutely customers” lists to minimize the false positives, reduce the burdens of the investigation staff, and maximize the entire process efficiency.

3.3 Transaction risks

Transaction risks can be summarized as three categories, which used as references for the People's Bank of China drawing up the determination criterion of suspicious transaction reports:

(1) *Fund-related behaviors.* Transactions that obviously involve with money-laundering activities or transactions that evidently cover the origin of funds. For example, internal transfers between different accounts under a same enterprise, rapid fund movement, and sudden activity of a previously dormant account.

(2) *Transaction-related behaviors.* Behaviors where transaction values exceed specified limits, or apparently structure the large-value funds into small amount of money (also called as smurfing), which should be paid to extra attentions. These behaviors normally pose higher risks of money-laundering suspicious activity, and are typically marked for further investigation.

(3) *Miscellaneous behaviors.* Frequent changes to an account can often be regarded as a signal that money laundering is taking place. Activities that would fall into this category include the settlement and/or standing instructions of an account, the movement of funds without a corresponding business, and the indirect deposit in excess of a designated amount into an account. These types of offsetting trades can increase the potential risk for money laundering.

3.4 Scenario detection

It refers to traditional monitoring systems utilizing a rules-based approach to detect known patterns of money-laundering behaviors. Scenario detection creates statistics data based on specific characteristics extracted from previous money-laundering cases, and interpret these data into a set of regular indicators. If the upper limits of these regular indicators are triggered, the information system will determine as "recurrence" of money-laundering activity, and giving an alert about the recurrence. Although scenario detection is still based on objective standards, it is a meaningful reference as well as an important component for risk-ranking process.

3.5 Behavior profiling

As traditional monitoring systems can only detect previously known suspicious behavior through building statistical profiles based on customer activities across all lines of business, and can be evaded from detection by money-launderers, behavior profiling becomes core module of the second-generation AML compliance system at the international level. Currently, only few companies have this technique, such as Fortent, and SAS. This module can anticipate the customer's next behavior tendency through the behavior profiling, generate continuous analysis and has the ability to learn and understand each individual customer profile, compare the real action with the expectation, and give an alert when the profiles thresholds are exceeded. In detail, profile engine can automatically self-update behavioral profiles for every account that is maintained. The system intelligently sifts through every transaction and analyzes behavior in the context of the behavioral profiles-on an individual basis, and against their defined peer group. When unusual or irregular activity is detected, alerts are triggered for investigation. Behavior profiling provides further analysis and allows a financial institution to discover previously unknown patterns of behavior through a compete knowledge of customer activity, and can even detect suspicious links between seemingly unrelated accounts.

3.6 Link analysis

As designed to identify hidden relationships amongst transaction, account, customer, and even associated organization, link analysis is a powerful tool for uncovering complex money-laundering operations. An effective link analysis module is tightly connected with "watch list module", conducting comprehensive analysis on the basis of truly valuable suspect information provided by law enforcement agencies at any time. When combating the financing of terrorism, link analysis module can point out high-risk geographic locations, which is a key element for risk-ranking process. In general, link analysis operates at three fundamental levels:

(1) *Business relationships.* The system should be able to identify potential account-holder, actual beneficial owner, and define unusual business relationships between underlying accounts, including relatives' relationship, affiliated company relationship, and special relationship with risk-sensitive persons.

(2) *Data consistency.* If money launderers attempt to disguise their behaviors by making changes of name, address, and reference details when opening accounts, the system should be able to identify the data inconsistency by checking other referencing data links, and generate alert reports about the inconsistent information.

(3) *Inter-related transaction.* A sophisticatedly designed money laundering *modus operandi* always involves in multiple financial institutions. The system should be capable of identifying possible associations through inter-related transaction patterns between accounts, both internal and external to the institution.

3.7 Risk ranking

It is a module that collects all the submitted risks from different risk assessment processes, and according to designed risk-weighted value, gives a final risk-ranking score for each transaction and its associated account, customer, and organization, and produces a suspects list ranked by their risk scores. Along with the suspects list, the system also gives reasonable grounds and explanations for each suspicious activity.

3.8 Workflow tools

Efficient workflow tools module is critical for the entire enterprise-wide AML solution. This process must be flexible, auditable, and have the ability to maintain, retrieve and report case management activities. It is the most important link which combines systems of the regulators and of other co-operated institutions together, and integrates all business links within an enterprise as an automatic solution body. The main functions of workflow tools are:

- *Information reporting and investigation.* Reporting system should provide an end-to-end AML SARs reporting process to the FIU, and in the meantime, guide the staff writing the filing report in "wizards" format, and encrypt the filings during the automatic delivery process. Investigating tool assists the compliance staff to further investigate and verify on the alerts submitted by the system before the filings are reported to the regulators. It also provides a summary of filing or reporting reasons, including account summary, customer background, current status, and transaction history. If necessary, visual or graphic documents can be supported for investigate the hidden relationship between different accounts.

- *Case management.* An effective case management can reduce false positives. It allows for the staff keep adding false-alert cases into the case library. Case management is helpful for the system learning new money-laundering rules, and is also useful for training staff about the enterprise's working process.
- *Record keeping.* This tool should meet key requirements of current international AML regulations, that is, all the transaction records generated over the previous five years at least should be kept as searchable data.

4. Conclusion

Traditional monitoring systems utilize a rules-based approach, designed to detect certain laundering behaviors rather than suspicious transactions. Rule-based detections are relatively easy to construct, inaccurate or unspecific rules, and tend to produce a high number of false positives. An enterprise-wide AML solution combines rules-based and advanced analytics to provide adequate protection from increasingly skilful money launderers, reduce the number of false positives which are labeled as risky transaction without genuine money-laundering risk, and determining previously unknown behavior patterns.

This paper explains key components of an enterprise-wide AML information system solution, including CDD, watch list, transaction risk, scenario detection, behavior profiling, link analysis, risk ranking, and workflow tools. However, in order to achieve the final success of AML combat, the enterprise-wide AML solution also needs supplementary supports from assistance of external environment, improvement of related regulatory guidance, maintenance of watch list database, and inter-relationship among different financial institutions. As a course which contains more public interests than private interests, AML works cannot be successfully accomplished without any of the above-mentioned elements.

References

FATF on Money Laundering (2007), *First Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism, People's Republic of China*, Financial Action Task Force on Money Laundering, Paris, June 29, p. 93.

FFIEC (2006), *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, Federal Financial Institutions Examination Council, Minneapolis, MN, p. 56.

Gao, Z.A. (2007), "Anti-money laundering: is suspicious reporting system effective?" ("反洗钱：可疑交易行为报告制度有效吗"), *Securities Market Guidance Paper* (*证券市场导报*), *Vol. 4* (*in Chinese*).

Kingdon, J. (2004), "AI fights money laundering", *IEEE Intelligent System*, Vol. 5, p. 87.

Shi, X.F. and Qiu, Z.Q. (2004), "Learning from American experience: improving Chinese AML system" ("借鉴美国经验，完善我国反洗钱体系"), *Theoretical World* (*理论纵横*), *Vol. 1, pp. 16-19* (*in Chinese*).

Shi, Y. (2007), "Analysis of over-reporting issue in Chinese suspicious activity reporting system" ("对我国可疑交易报告数量增长过快的分析"), *Chinese Finance* (*中国金融*), *Vol. 19, pp. 44-5* (*in Chinese*).

Tang, J. (2005), "Customer behavior-based AML monitoring and analysis system" ("基于客户行为模式识别的反洗钱监测与分析体系"), *Journal of Zhongnan University of Economics and Law* (*中南财经政法大学学报*), *Vol. 4, pp. 62-7* (*in Chinese*).

Yang, S. and Wang, P. (2005), "Data-mining based RMB anti-money laundering system" ("基于数据挖掘技术的人民币反洗钱系统设计"), *Financial Theory and Practice* (*财经理论与实践*), *Vol. 26, pp. 105-9* (*in Chinese*).

Zhang, C.H., Sun, Y.Y. and Yao, W.H. (2006), "Determination of individual suspicious transaction based on cluster analysis" ("基于聚类分析的个人可疑交易识别研究"), *Electronic Finance* (*金融电子化*), *Vol. 5, pp. 195-8* (*in Chinese*).

Further reading

Kini, S. (2005), "Federal bank regulatory agencies issue long-awaited anti-money laundering examination manual", *The Banking Law Journal*, Vol. 122 No. 9, pp. 940-52.

Corresponding author

Lishan Ai can be contacted at: ali_shane1127@hotmail.com