Study on the Design of the Tool for Assessment of Security Risks of the Tasks for Prevention of Money Laundering at Financial Companies

PillJung Kim¹, HyungMin Lim² and SeokYoon Kim³

¹, ²Korea
(E-mail: pjkim@lnjtech.co.kr, hmlim@lnjtech.co.kr)
³ Korea
(E-mail: ksy@ssu.ac.kr)

ABSTRACT The tasks for prevention of money laundering are currently carried out by the method to provide the information potentially related to money laundering to the law enforcement agencies through the business cooperation between Financial Intelligence Unit (FIU) and the financial companies. The details of transactions executed at the financial companies inevitably include the sensitive information of the individuals in most cases. Therefore, the security of information is very critical but there is no coverage of the information security requirements addressed in the FATF recommendations. In addition, under the current circumstances, most of the supervisory institutions of financial companies do not extend their regulations on information security to the scope of the tasks for prevention of money laundering performed within the internal networks of the financial companies. Accordingly, the tasks for prevention of money laundering can be associated with the problem of being placed in the blind area of security. In order to solve this problem, this thesis proposes the method to design the customized tool for assessment of security risks on the basis of the indicator for assessment of security risks identified after defining the business model for prevention of money laundering at financial companies.

Keywords: Money Laundering, Prevention of Money Laundering, FATF, Security Risk Assessment, Mutual Evaluation

1. INTRODUCTION

The tasks for prevention of money laundering are being performed based on the business cooperation between each financial company such as the banks, security companies and others and the law enforcement agencies such as the Public Prosecutors' Office, the National Police Agency, the National Tax Service and others under the lead of Financial Intelligence Unit (FIU).

The financial companies prepare the reports of the transactions involving a large amount of cash or suspicious details and transfer them to Financial Intelligence Unit (FIU). The Financial Intelligence Unit (FIU) conducts the examination of the transactions included in the reports and notifies the results to the law enforcement agencies in the relevant areas, which launch the investigation on a full-fledged scale. The overall business scheme aims to eradicate the possibility of money laundering by the decision whether to prosecute based on the result of the investigation.

Since the reports prepared include the sensitive information of the parties executing the transactions, the security management of the channel for reporting is of significant importance but the security protection is seriously vulnerable under the current circumstances due to the lack of considerations given to the security implications.

Based on this, the current thesis proposes the method for design of the tool for assessment of security risks which will support the financial companies in their secure performance of the tasks for prevention of money laundering.
The composition of this thesis is as follows. Following the introduction, the theoretical background of the technology applicable in the field of money laundering is explained and the concrete details of the method being proposed are explained in 2. *SUGGESTED TOOL DESIGN* and the conclusion is drawn.

## 2. *SUGGESTED TOOL DESIGN*

The system for prevention of money laundering involves the establishment of the sound order in financial transactions by preventing the laundering of crime funds through the financial institutions and others and the establishment and operation of the comprehensive management system connecting among the financial systems, jurisdictional systems and the international schemes for cooperation with the aim to prevent the propagation of grave crimes such as the organizational crimes, drug crimes and others.

### 2.1. **Business Model**

The tasks for prevention of money laundering are customarily implemented based on the business model including the 7 types of processes as follows.

![Figure 1. Business Model](image)

The first step is where the transactions are executed and the information about the transactions executed at the branches of the financial companies is transmitted to the business and AML systems at the head office. The second step involves the request for re-verification of the reported information and enables the query view of the transaction information analyzed in the AML system for re-verification by the employees at the counters of sales offices. The third step is the monitoring stage where the review and judgment by the personnel in charge at the head office are requested with the delivery of information requiring the decision, such as analyzed STR transmitted from AML and others. The fourth step has to do with the transmission of the result of re-verification by the sales offices whereby the report information received from the AML system is re-verified at the sales offices with the results transmitted to the personnel in charge of reporting at the head office and the fifth step involves another monitoring activity to identify and communicate any pieces of information missing during the re-verification at the sales offices. And the details for reporting are submitted to Financial Intelligence Unit (FIU) at last in the sixth step. In addition, any data necessary in addition during the examination and analysis at Financial Intelligence Unit (FIU) is requested to the compliance officer at the head office and the replies are received in the seventh step.
2.2. The Proposed Design

On the basis of the above business model, the indicator for assessment of security risks was established based on the following methodology.

1. Derivation of penetration factors (threats, vulnerabilities and possibility of occurrence) at each step.
2. The extent of riskiness is determined based on the evaluation of the penetration factors derived.
3. Formulation of a checklist with the penetration factors and determination of the indicator by assigning the grades depending on the extent of riskiness.

Since the indicator determined in this way allows the evaluation and management of the risks in customization to the environment of the financial companies, each financial company should assess the security risks internally every year. However, the compliance itself is difficult in general due to the lack of security human resources in the part for prevention of money laundering of the financial companies and other reasons. Given these considerations, the design of tool is proposed in this thesis to enable the effective and easy assessment of security risks in customization to each financial company.

The tool for assessment of security risks comprises five parts as follows.

In the input part, the indicator for assessment of security risks and the current status information are entered to enable the utilization of those data at the time of risk assessment. In addition the security budget and the improvements achieved based on the result of risk assessment are arranged to be entered and received to allow the continuous updates.

The process part can be divided into two subparts including the one for assessment of risks and the other for operations. In the subpart for assessment of risks, the risk assessment is conducted based on the data entered in the input part and the status of improvements is managed. In this way, the improvements and the results of risk assessment can be made up-to-date on a real-time basis. In the subpart for operations, the data for reporting to Financial Intelligence Unit (FIU) is refined and managed.

In the output part, the results of processing in the process part are consolidated into a report to allow the clear confirmation by each related personnel and the improvement is allowed in the security standards and indicators thereby aiding with the propagation of security controls based on the results of risk assessment to their corresponding parts in the form of clear documents.

In the review part, the feedback is allowed based on the review of each type of reports prepared in the output part by each related personnel and the reporting part was designed to enable the proposed system to submit the report to Financial Intelligence Unit (FIU) on a timely basis based on the result of review.
3. CONCLUSION

This thesis proposed the design of tool for assessment of security risks in a move to suggest the measures to effectively reinforce the security of tasks for prevention of money laundering which deal with critical information.

By conducting the assessment of security risks by utilizing the corresponding tool for assessment of risks, the following three effects can be anticipated.

1. The security can be reinforced in a customized pattern for each financial company,
2. The security can be reinforced conveniently with a small number of human resources as the method utilizes an automated tool, and
3. The continuous reinforcement of security can be allowed through the conduct of internal assessment of risks each year.

Moreover, by enabling the periodical and effective security assessment by the domestic financial companies, the illegal money laundering of colossal sizes can be blocked safely with the possibility for further contribution to the national competitiveness and security.

REFERENCES