Knowledge Sharing Program

2012 Modularization of Korea's Development Experience:

Experiences and Methodology of Korea's Anti-Money Laundering System Deployment and Development

2013

FINANCIAL SERVICES COMMISSION

SAMIL | Samil PricewaterhouseCoopers

2012 Modularization of Korea's Development Experience:

Experiences and Methodology of Korea's Anti-Money Laundering System Deployment and Development

2012 Modularization of Korea's Development Experience

Experiences and Methodology of Korea's Anti-Money Laundering System Deployment and Development

Title	Experiences and Methodology of Korea's Anti-Money Laundering System Deployment and Development
Supervised by	Financial Services Commission, Republic of Korea
Prepared by	Samil PricewaterhouseCoopers
Author	Chang-Joo Lee, Samil PricewaterhouseCoopers, Director Jin-Chun Lee, Samil PricewaterhouseCoopers Consulting, Senior Manager
Advisory	Chul-Hwan Lee, Korea Institute of Finance, Non-standing Commissioner (Former KoFIU's Commissioner)
Research Management	KDI School of Public Policy and Management
Supported by	Ministry of Strategy and Finance (MOSF), Republic of Korea

Government Publications Registration Number 11-7003625-000027-01

ISBN 979-11-5545-046-8 94320

ISBN 979-11-5545-032-1 [SET 42]

Knowledge
Sharing
Program

Government Publications Registration Number

11-7003625-000027-01

Knowledge Sharing Program

2012 Modularization of Korea's Development Experience

Experiences and Methodology of Korea's Anti-Money Laundering System Deployment and Development

FINANCIAL SERVICES COMMISSION

SAMIL | Samil PricewaterhouseCoopers

Preface

The study of Korea's economic and social transformation offers a unique opportunity to better understand the factors that drive development. Within one generation, Korea has transformed itself from a poor agrarian society to a modern industrial nation, a feat never seen before. What makes Korea's experience so unique is that its rapid economic development was relatively broad-based, meaning that the fruits of Korea's rapid growth were shared by many. The challenge of course is unlocking the secrets behind Korea's rapid and broad-based development, which can offer invaluable insights and lessons and knowledge that can be shared with the rest of the international community.

Recognizing this, the Korean Ministry of Strategy and Finance (MOSF) and the Korea Development Institute (KDI) launched the Knowledge Sharing Program (KSP) in 2004 to share Korea's development experience and to assist its developing country partners. The body of work presented in this volume is part of a greater initiative launched in 2010 to systematically research and document Korea's development experience and to deliver standardized content as case studies. The goal of this undertaking is to offer a deeper and wider understanding of Korea's development experience with the hope that Korea's past can offer lessons for developing countries in search of sustainable and broad-based development. This is a continuation of a multi-year undertaking to study and document Korea's development experience, and it builds on the 40 case studies completed in 2011. Here, we present 41 new studies that explore various development-oriented themes such as industrialization, energy, human resource development, government administration, Information and Communication Technology (ICT), agricultural development, land development, and environment.

In presenting these new studies, I would like to take this opportunity to express my gratitude to all those involved in this great undertaking. It was through their hard work and commitment that made this possible. Foremost, I would like to thank the Ministry of Strategy and Finance for their encouragement and full support of this project. I especially would like to thank the KSP Executive Committee, composed of related ministries/departments, and the various Korean research institutes, for their involvement and the invaluable role they played in bringing this project together. I would also like to thank all the former public officials and senior practitioners for lending their time, keen insights and expertise in preparation of the case studies.

Indeed, the successful completion of the case studies was made possible by the dedication of the researchers from the public sector and academia involved in conducting the studies, which I believe will go a long way in advancing knowledge on not only Korea's own development but also development in general. Lastly, I would like to express my gratitude to Professor Joon-Kyung Kim and Professor Dong-Young Kim for his stewardship of this enterprise, and to the Development Research Team for their hard work and dedication in successfully managing and completing this project.

As always, the views and opinions expressed by the authors in the body of work presented here do not necessary represent those of the KDI School of Public Policy and Management.

May 2013

Joohoon Kim

Acting President

KDI School of Public Policy and Management

Contents | LIST OF CHAPTERS

Chapter 2

Contents | LIST OF CHAPTERS

Contents | LIST OF TABLES

Chapter 1

Chapter 2

Contents | LIST OF TABLES

Chapter 3

Contents | LIST OF FIGURES

Chapter 1

Chapter 2

Chapter 3

Contents | LIST OF FIGURES

Summary

In today's global economic conditions, the economy of one country is inextricably linked to another in various ways. The wave of liberalization in several sectors including trade, financing, and capital led by major developed countries from the 1970s gained momentum as information technology developed at a breakneck pace from the 1980s up until today. Liberalization expanded to agriculture, finance, medicine, and education, thus resulting in a rapid increasing scale and frequency of capital flows compared to the past capital flows (borrowing from '2.2.1 Background of AML System').

To fight money laundering and tax evasion accompanied by rapid changes in global economic conditions, Korea enacted and enforced the Presidential Financial and Economic Emergency Order on Real Name Financial Transactions and Guarantee of Secrecy of 1993, the Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics, etc. of 1995, and the Act on Special Cases Concerning Forfeiture for Offences by Public Officials of 1995. The Acts, however, stipulated the scope of predicate offences for the forfeiture of illegal proceeds and drug trafficking related crimes, so they did not meet international AML standards. After that, with the need for the AML framework led by international communities, including the UN and the liberalization of foreign exchange transactions, Korea adopted an institutional framework for anti-money laundering (AML) by enacting a law in 2001. Since the adoption of the AML framework in 2001, the Korean government established AML related laws, regulations, and systems in order to urge financial institutions to adopt regulation based systems until the enhanced AML Framework in 2007. After the enhanced AML framework was adopted in 2007, the government introduced a rule-based risk management system, organizing the system and establishing the related system to leverage financial institutions as the starting point for anti-money laundering. Accordingly, this helped fulfill the 'international Anti-money Laundering/Combating the Financing of Terrorism (AML/CFT) standards.' Since 2001, the AML regime and its related system have brought changes in Korea through evolutionary developments: Korea improved its national confidence domestically and enhanced the transparency of financial transactions internationally by enhancing its transparency of fund transactions, taking active participation in AML activities led by international institutions and playing a leading role in the Asia-Pacific region. This research focuses more on the successful adoption of the AML System for information processing and analysis, implementation progress and the strategic achievements in accordance with the adoption of AML regime, and less on the details of the AML system.

In relation to the establishment and operation of the FIU Information System, this research provides background on the system adoption, implementation strategies and progress, success factors, and improvements. First of all, the background explores the changes in the international organizations such as the FATF and the Egmont Group associated with AML activities, and discusses the adoption of Korea's AML regime. Implementation strategies of the Financial Intelligence Unit (FIU) Information System describes the implementation strategies for each stage, and specifies implementation objectives for each stage such as the base for information analysis, risk-based evaluation analysis, usage of accumulated information, and supervision of financial institutions.

The following implementation progress section examines the establishment progress of KoFIU's FIU Information System, conducted by six projects, with a summary of the establishment, implementation details, achievements, and improvements of each project.

Finally, references are provided for other countries to adopt an AML regime and establish an information system by reviewing the adoption of Korea's AML framework and the establishment process of an information system.

Chapter 1

Background of Anti-Money Laundering Framework

Background of Anti-Money Laundering Framework

1. International AML Framework

1.1. Effects of Money Laundering

In general, money laundering (ML) is the process of concealing illicit gains generated from criminal activities such as drug trafficking, organized crime and disguising illegal proceeds as legitimate assets. Money laundering is used to launder not only ill-gotten gains from organized crime including arms trade, smuggling, drug trafficking and prostitution, but also from illicit funds by corruption offences including embezzlement, bribery, political commission, insider trading, and computer fraud.

The generally accepted definition of money laundering is "the process of disguising the illegal origin of funds in order to make them appear legitimate."[1] The term stems from the process of avoiding funds-tracking during the 1920s when criminal organizations such as Al Capone disguised ill-gotten gains from gambling or illicit liquor trafficking as legitimate income from "laundries" under their control with frequent cash transactions.

In Korea, the term money laundering was generally used when it adopted the real-name financial transaction in order to freeze the underground loan market in the 1980s and 1990s. It is defined as "an act to disguise the acquisition and disposal of illicit gains; or conceal the assets and disguise the acquisition and disposal of assets for the purpose of tax evasion by means of

1. 1985, by the United States, President's Commission on Organized Crime.

foreign exchange transactions or conceal the assets."[2] Korea, unlike foreign countries, typically includes foreign exchange transactions for the purpose of tax evasion as money laundering.

The size of money laundering is identified by a micro methodology based on information from law enforcement agencies such as investigation materials or trial ones. The macro methodology is based on macro-economic indicators, including currency data or taxation reference. However, because money laundering takes place secretly, accurate estimates are virtually impossible to produce.

The 1987 the United Nations (UN) report estimated that the size of global drug transactions based on the annual drug production reached $300 billion. In 1994, the UK's *Financial Times* reported that the amount of annual money laundering in the world was roughly $500 billion—equivalent to 2% of world's GDP.

According to John Walker's research in 1998, the size of money laundering in the world was about $2.85 trillion with $1.32 trillion of money laundering occurring in the United States per year. The inflows of money laundering into the United States amounted to about $540 billion. Additionally, the amount of money laundered in Korea was roughly $21.2 billion.

Money laundering is practiced on a worldwide scale. Furthermore, the scheme of money laundering is globalized and internationalized through financial institutions, internet, transactions, and underground networks, leading to the disruption of the international financial system as well as associating with the terrorist organization. This explains why money laundering is a matter of concern.

The social and economic effects of money laundering are as follows:

① Social Aspect

If money laundering is ignored, it can pose a significant social and political threat. Money laundering could undermine social solidarity and ethical standards for society as a whole, ultimately weakening the democratic system. For instance, a bloated criminal organization using money laundering could control a larger pie of the economy by making a business investment through financial institutions and to a larger extent control governmental functions by influencing public officials and the government. In addition, since the act of money laundering is closely linked to criminal activities, there is a vicious cycle in which laundering funds are used to finance new crime.

2. Article 2-4 of the Financial Traction Reports Act (FTRA) and Article 3 of the Proceeds of Crime Act Meanwhile, Rick McDonell, Head of the Asia/Pacific Group on Money Laundering (APG) Secretariat, who attended the Asian Development Bank (ADB) Annual Forum held in Hawaii on May 7, 2001, announced that the amount of money laundered globally was roughly $1 trillion, of which the amount of $200 billion to $300 billion was laundered in the Asia Pacific region only.

② Economic Aspect

Money laundering can have a very significant influence on financial institutions. For instance, if it is easier for criminal organizations to make criminal earnings legitimate by bribing financial institutions' employees, financial institutions can be a part of the criminal network serving as an accomplice. This could lead to an increased risk of the soundness of the financial institution and undermine the financial institution's reputation if there is any evidence of conspiracy with the criminal organization.

If the financing of terrorism through an overseas bank branch occurs and the funds are actually used to carry out terrorist activities, the bank could tarnish its reputation and it would serve as a heavy blow to its management capability. Furthermore, operating activities such as suspension of transaction may follow.

As with the financial crisis in Russia at the end of the 1990s, the influence of organized crime on a country's economy and financial circumstances could have devastating consequences in foreign investment and international money transactions. If governments with off-shore financing centers take slow countermeasures, the risk of money laundering will be increased.

Macroeconomic effects of money laundering are diverse. First, money laundering prevents a country from establishing economic policies since it is hard to estimate economic indicators such as currency volume, inflation level, and interest rate fluctuations.

Second, temporary cross-border transfers of funds can increase fluctuations in exchange rates and interest rates. To understand movements of currency, it is necessary to locate the whereabouts of currency issuing nations and depositors. In this regard, if the data of money transfers from one country to another is distorted, it is harder to trace the total volume of money, thereby impacting interest rates and exchange rates.

Third, the contamination effect of money laundering disrupts legitimate transactions. If countries, like Russia, are viewed as a money laundering country, they could be subject to tacit restraints on legitimate transactions since their legitimate transactions are regarded as suspicious.

1.2. Establishment of International AML Standards

In order to combat narcotic crimes countries including the United States, the United Kingdom, and Australia enacted a legislation governing the criminalization of laundering of drug-related proceeds in the 1970s. With the prevalence of grave crimes such as drug trafficking at the international level, countries began to recognize the need for mutual cooperation in criminal investigation. In addition, in an attempt to build confidence in international financial institutions in line with the liberalization of the financial market, countries raised awareness on preventing money laundering through the banking system. In other words, there was widespread awareness that anti-money laundering is a prerequisite for not only eradicating grave crimes, including drug-related crimes, but also for establishing a sound banking system. Accordingly, there was a growing demand for adopting legislation that all serious crimes are predicate offences of money laundering. In response to the demand, the international AML standards were established.

The establishment process of international AML standards consist of three stages: the individual response before signing major international conventions; the establishment of an initial international convention; and the establishment of international standards through international organizations after the 1990s.

① Individual Countries' Response

Since the 1970s, the United States showed interest in drug-related money laundering. In the 1980s, the United States, the United Kingdom, and Australia implemented money laundering related laws. At the international level, the Committee of the Council of Europe began to discuss the money laundering problem for the first time and announced the *Measures Against the Transfer and Safekeeping of Funds of Criminal Origin* on June 27, 1980.

② Initial Major International Conventions

From the end of the 1980s through the early 1990s, the international community took collective measures in response to the concern about drug-related money laundering. In 1988, the United Nations (UN) signed the *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)*, which criminalizes drug-related criminal funds laundering and confiscates the funds. In addition, in December of 1988, the Basel Committee on Banking Supervision (Basel Committee), of the Bank for International Settlements (BIS) issued the *Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention)*. Meanwhile, the Council of Europe adopted the *Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime* in Strasbourg, France on November 8, 1990.

③ Establishment of International Standards through International Organizations

In response to drug-related money laundering, the G-7 countries formed the Financial Action Task Force on Money Laundering (FATF) in 1989 and published a set of 40 recommendations, *The Forty Recommendations on Money Laundering (The Forty Recommendations)*. The Forty Recommendations have been revised to take account of increasingly sophisticated and complicated money laundering methods. In June 1996, the first revision of the Forty Recommendations included a wide range of serious crimes except drug crime as money laundering predicate offences. As all other serious crimes as well as drug-related crimes are committed internationally and collectively, this reflects the need for expanding the scope of predicate offences for money laundering and the mutual legal assistance, such as criminal investigations.

In 1997, the Egmont Group of Financial Intelligence Units (Egmont Group) set "the definition of a Financial Intelligence Unit (FIU)," which is a body unit for effectively and systematically dealing with money laundering information, at the 5th plenary session in order to build mutual assistance and enhance the role of supporting the establishment of the FIU.

Furthermore, the terrorist attacks in the United States on September 11, 2001 paved the way for strong international AML standards. The events increased the importance of an AML framework for combating terrorism and the need for establishing the AML framework based on international assistance. In this context, the FATF on October 30, 2001 adopted the eight *Special Recommendations on Terrorist Financing (Special Recommendations)* to combat the financing of terrorism (CFT). In October 2004, the FATF added a provision to the Special Recommendations to deter cash couriers widely used for financing terrorists at its plenary meeting and the Special Recommendations became the *9 Special Recommendations*.

Although not binding as law among member countries, the FATF Special Recommendations, which serve as international standards for providing legislative measures for members, are de facto binding through the fulfillment of the FATF members, the classification of the Non-Cooperative Countries and Territories (NCCT) against money laundering.[3] Currently, the FATF Special Recommendations have been effectively adopted and carried out.

1.3. International Organization's Establishment and Main Activities

There are major international organizations associated with anti-money laundering: the FATF, the Egmont Group, and the APG (Asia/Pacific Group on Money Laundering). In addition, the IMF (International Monetary Fund)/WB (World Bank) and the UN are working together against money laundering.

3. The Philippines was scheduled to hold the plenary meeting of the APG in 2003 but after it was designated as the NCCT country, it failed to make progress on its deficiencies. As a result, the Philippines withdrew its right to hold the plenary meeting and passed AML-related legislation, which had been long delayed, for fear of counter-measures that would be taken by the FATF.

The FATF is currently comprised of 34 member jurisdictions and 2 regional organizations as of September 2012. Shown in 〈Table 1-1〉, the membership is composed of 34 countries, among which are 26 OECD member countries and 8 non-OECD countries, and two organizations: the European Commission and the Gulf Co-operation Council. Poland, Hungary, the Czech Republic, Slovakia, Chile, Israel and Slovenia are the seven OECD member countries that are not FATF members.

1.3.1. Financial Action Task Force on Money Laundering (FATF)

The Financial Action Task Force on Money Laundering (FATF), which is a typical body for anti-money laundering (AML), was established in 1989 at the Group of Seven (G-7) Summit in Paris, as there was growing recognition among the G7 leaders of the importance of mutual cooperation in AML. The FATF was initially a temporary body that extended its term every five years. Later, the FATF evolved into a permanent body with an eight year life span in February 2004 at the plenary meeting, as it played an important role in global CFT activities following the events of September 11, 2001.

The FATF is an intergovernmental body that provides international standards for anti-money laundering (AML) and combating the financing of terrorism (CFT). It also develops and promotes policies. The purpose is to prevent criminal proceeds from being used for criminal activities in the future and to promote legitimate economic activities.

a. Main Activities

In recent years, in order to establish a global AML network due to an increasing number of members and the reinforcement of the FATF-style regional bodies, the FATF, which departed from its position before, decided to accept Russia and South Africa as new members in the 2002 plenary session. Moreover, the FATF is showing signs of its intention to include new members in the near future. Korea became an associate member in August 2006 and a full member of the FATF in October 2009 through mutual evaluation.

Table 1-1 | FATF Members

Region	Number of Countries	OECD Member Countries	Non-OECD Countries	International Organization
Europe	20	Greece, Kingdom of the Netherlands, Norway, Denmark, Germany, Luxemburg, Belgium, Sweden, Switzerland, Spain, Iceland, Ireland, United Kingdom, Austria, Italy, Portugal, France, Finland	Russia	European Commission
America /Others	7	United States, Mexico, Canada	South Africa, Brazil, Argentina,	Gulf Cooperation Council (GCC)
Asia /Pacific	9	New Zealand, Japan, Turkey, South Korea, Australia	Singapore, India, China, Hong Kong	
Total	36	26	8	2

Source: The Financial Services Commission

The activities of the FATF are summarized as follows:

① Establishing a global network for Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT)

② Setting the FATF recommendations, an international AML/CFT standard, and evaluating and monitoring their implementation

- Evaluating the implementation of international AML/CFT standards (mutual evaluations)

- Imposing sanctions on countries not fulfilling the standard and encouraging the countries concerned to adopt AML-related legislation/system

③ Researching AML/CFT techniques and developing counter-measures

The FATF calls on member countries and non-member countries to implement the Forty Recommendations, monitors members' progress in implementing AML frameworks through annual self-assessments and mutual evaluations, and imposes sanctions on countries that are ill-equipped or are not cooperative in AML frameworks by designating the countries as Non-cooperative Countries and Territories (NCCT's). With regard to an NCCT, according to the FATF Recommendation 21, financial institutions of member countries must pay special attention to business relationships and transactions with natural or legal persons and financial institutions from countries and territories recorded on the NCCT list. In addition, in the event an NCCT country does not make sufficient progress, further counter-measures may be imposed. The counter-measures consist of: ① stringent requirements to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries; ② rejecting approval when considering requests for approving the establishment in FATF member countries of subsidiaries, branches or representative offices of banks, if the relevant bank is from an NCCT; ③ Reporting of financial transactions with such countries; and ④ Warning non-financial sector businesses that transactions with entities within the NCCTs might run the risk of money laundering. For example, as a non-member, Nauru was listed as an NCCT and was devastated under the sanction.

The FATF reviewed 26 countries for NCCT on February 26, 2000 and 15 countries were announced as NCCT in June 2000 at the FATF plenary. There has been listing and de-listing in the framework for the NCCT initiative by continuous monitoring on whether a country listed as NCCT makes sufficient progress in remedying its deficiencies. As of October 2006, there were no non-cooperative countries and territories in the context of the NCCT initiative. The history of listing and de-listing countries is shown in <Table 1-2>.

Table 1-2 | Designation of Non-Cooperative Countries and Territories Concerning Anti-Money Laundering

Month/Year	Number of NCCT	Designation of NCCT
June/2000	15	• Announcement of 15 NCCT-listed countries after reviewing 26 countries ▷ Russia, Liechtenstein, Philippines, Israel, Lebanon, Panama, Dominica, Bahamas, Cayman Islands, Cook Islands, Marshall Islands, Nauru, Niue, St. Kitts and Nevis, St. Vincent and Grenadines
June/2001	17	• Excluded Country (4): Liechtenstein, Panama, Bahamas, Cayman Islands • Included Country (6): Hungary, Guatemala, Myanmar, Egypt, Nigeria, Indonesia
September/2001	19	• Included Country (2): Grenada, Ukraine
June/2002	15	• Excluded Country (4): Hungary, Israel, Lebanon, St. Kitts and Nevis
October/2002	11	• Excluded Country (4): Russia, Dominica, Niue, Marshall Islands
February/2003	10	• Excluded Country (1): Grenada
June/2003	9	• Excluded Country (1): St. Vincent and Grenadines
February/2004	7	• Excluded Country (2): Egypt, Ukraine
June/2004	6	• Excluded Country (1): Guatemala ▷ NCCT: Indonesia, Philippines, Myanmar, Nigeria, Nauru, Cook Islands
February/2005	3	• Excluded Country (3): Indonesia, Philippines, Cook Islands
October/2005	2	• Excluded Country (1): Nauru
June/2006	1	• Excluded Country (1): Nigeria
October/2006	0	• Excluded Country (1): Myanmar

Source: Financial Action Task Force on Money Laundering

b. FATF 40 Recommendations

a) 40 Recommendations on Money Laundering (40 Recommendations)

The FATF has adopted a set of 40 Recommendations, which was initially developed in 1990. The 40 Recommendations provide a complete set of counter-measures against money laundering (ML) consisting of: organizing the criminal justice system and law enforcement; enhancing the financial system and regulation; and fostering international cooperation. As money laundering methods grow sophisticated and complex, the recommendations have been revised to take into account changes in money laundering trends.

The first revision of the Recommendations in 1996 consisted of: expanding the applicable scope of predicate offences of money laundering to include other serious crimes; obligating financial institutions to report suspicious transactions; and strengthening customer identification on legal persons.

The second revision of the Recommendations adopted in June 2003 at the Berlin plenary consisted of: ① expanding the scope of predicate offenses to include 20 criminal offences such as organized crime, terrorism, human trafficking and illicit trafficking in narcotic drugs ② encompassing Customer Due Diligence (CDD) in the context of implementing AML obligations to identify and verify the beneficial owners and to regulate the CDD process ③ expanding the scope of AML obligations only applied to financial institutions to include non-financial businesses and professions such as lawyers, accountants, casinos, real estate agents, and precious metal dealers.

The third revision of the Recommendations announced on February 16, 2012 at the headquarters of OECD in Paris contain: ① adopting a risk-based approach, which provides enhanced measures depending on the risk levels of money laundering; and ② imposing financially specific counter-measures against the proliferation of Weapons of Mass Destruction (WMD) and preventing/combating/banning terrorists financing. The contents of the revisions are shown in <Table 1-3>.

Table 1-3 | Revisions of the 40 Recommendations on Money Laundering

Revision No.	Year	Main Contents of Revision
1st	1996	• Including a wide range of predicate offences of money (drug trafficking → serious crimes) • Obligating financial institutions to report suspicious transactions • Strengthening customer identification on legal persons
2nd	2003	• Establishing new regulation on the financing of terrorism • Imposing AML obligations on non-financial businesses·professions • Requiring each country to establish an FIU
3th	2012	• Adopting a risk-based approach • Instituting financially specified counter-measures against the proliferation of Weapons of Mass Destruction

Source: Korea Financial Intelligence Unit

b) Eight Special Recommendations on Terrorist Financing

A Counter-Terrorism Financing (CFT) regime, which was adopted following the events of September 11, 2001, criminalizes financing terrorists according to the *UN Convention for the Suppression of the Financing of Terrorism* (1999) and carries out the process of identification, search, seizure and confiscation. The FATF adopted the CFT regime as the FATF standards, or its Special Recommendations at an emergency plenary session in Washington between October 29, 2001 and October 30, 2001. The Eight Special Recommendations at their early form are as follows:

① Implementing the UN resolutions on combating the financing of terrorism

② Criminalizing the financing of terrorism

③ Freezing and confiscating terrorist assets

④ Reporting terrorist-related funds of institutions responsible for AML obligations

⑤ Working on mutual legal assistance mechanisms and having the procedures of extradition in place

⑥ Registering individuals or legal entities that provide money remittance or transfer services and implementing the FATF Recommendations on banks and non-bank financial institutions

⑦ Retaining accurate information on the funds transfer of financial institutions

⑧ Reviewing law and regulations on CFT and paying attention to non-profit organizations

The FATF called for its members to carry out self-assessments for the Special Recommendations on combating the financing of terrorism by December 31, 2001 and implemented them by June 2002. In addition, the FATF members are required to make regular announcements of the total amount of terrorist funds frozen in accordance with the U.N. Security Council Resolution (UNSCR).

In October 2002, both the FATF members and non-member countries published self-assessments at a FATF plenary session. The contents of non-compliance with the requirement involved criminalizing CFT and obligating the reporting of suspicious transactions to terrorist funds.

In October 2004, the FATF added a provision on cash couriers widely used for terrorist financing at the plenary session and adopted *Nine Special Recommendations*. The objective of the *Nine Special Recommendations* is to ensure that each country provides competent authorities such as customs with legal authority to detect the physical cross-border transportation of currency and bearer negotiable instruments, restrain currency and bearer negotiable instruments that are either suspected of being related to terrorist financing or misrepresented in a required declaration and confiscate currency and bearer negotiable instruments that are related to terrorist financing or money laundering.

In recent years, the FATF has incorporated CFT, which is its main task of the Recommendations, into the 40 Recommendations. This reflects that the CFT framework is closely linked to AML measures.

c. Third Revision of the 40 Recommendations

The FATF published the revised FATF Recommendations on February 16, 2012 at 11 AM, in OECD headquarters of Paris. There are growing threats of money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction that can destabilize and destroy the development and transparency of the financial system. In response, the FATF international standard was revised to enhance the transparency of the international financial system and global safety network and imposed counter-measures against corruption and tax evasion that were urgently needed. One of the distinct characteristics of the third revision is that it reflects the comprehensive opinions from private interests and civic society through a private sector consultative forum. The contents of the third revision are as follows:

First, the FATF established the risk-based approach by applying enhanced measures where the risks are higher with the option of simplified measures where the risks are lower. In other words, the risk-based approach enables financial institutions to carry out self-assessment of money laundering risks, such as customers, goods and services and to apply the enhanced measures based on the nature of the risks. Therefore, financial institutions and other designated sectors were allowed to focus more on resources with higher risk areas.

Second, the FATF strengthened transparency requirements for the beneficial ownership control of companies and the parties to wire transfers. Since lack of transparency on the ownership and control of legal persons and legal arrangements, or on the parties who conduct wire transfers makes those instruments vulnerable to misuse by criminals and terrorists, the FATF strengthened requirements that there should be reliable information available about the beneficial ownership and control of companies, trusts and other legal persons or legal arrangements. In addition, there are rigorous requirements for information necessary for wire transfers. Measures to improve transparency, implemented on a global basis, will make it difficult for the criminals and terrorists to conceal their activities.

Third, the FATF expanded the scope of international cooperation. In response to growing money laundering and terrorist financing threats at the international level, the FATF expanded the scope and application of international cooperation between authorities and financial institutions. This provided more effective exchanges of information for investigative, supervisory, and prosecutorial purposes as well as assisting countries in tracing, freezing, and confiscating illegal assets.

Forth, in order to put top priority and tackle new and aggravated threats and agendas set by the international community, including the G20, the FATF came up with the following three measures.

① The FATF adopted a new Recommendation on the financing of the proliferation of WMD to implement consistent and effective targeted financial sanctions upon the request of the UN Security Council. The FATF froze the assets of the natural or legal persons related to the proliferation of WMD designated under the UN Security Council Resolutions. As of February 2012, the individuals include 41 Iranians and 5 North Koreans. There are 75 Iran-related groups and 8 North Korea-related groups.

② The FATF Recommendations strengthen the requirements of financial institutions to identify politically exposed persons (PEPs) – who represent administrative·judicial·military officials, senior politicians, and senior executives of state owned corporations. Financial institutions are required to identify whether customers are PEPs and implement "enhanced customer due diligence (CDD)" process if transactions with domestic PEPs have higher risks. Korea adopted the "enhanced CDD" in 2008.

③ Fiscal crimes are classified as money laundering predicate offences. Thus, this enables Korea to take preventive and judicial measures for anti-money laundering against the proceeds of tax-related crimes. Furthermore, the smuggling offence has also been clarified to be included in predicate offences related to customs and excise duties and taxes.

Fifth, terrorist financing remains a major priority for the FATF Recommendations. Thus, this revision made it possible to integrate the FATF's Nine Special Recommendations on terrorist financing into the Forty Recommendations. This reflects that terrorist financing is not a temporary concern and that countermeasures against terrorist financing are closely related to those against money laundering.

Sixth, the FATF clarified requirements of financial institutions by taking account of recent trends in the financial sector. For instance, the FATF reflected experiences learned from the implementation of the Recommendations by each country, such as by specifying customer due-diligence requirements, to help assist countries that had practical difficulties in implementing CDD.

<Table 1-4> represents the structure of the third revision and the relationship between the third revision and the second revision of the FATF Recommendations.

Table 1-4 | Structure of the Third FATF Recommendations and the Relation with the Second Revision

Category	Subcategory	No.	Recommendations	Second Revision Reference
AML/CFT Policy and Coordination		1	Application of risk assessment and risk-based approach	New recommendation
		2	Cross-border cooperation and coordination	R.31
Legal system related to Money Laundering and Confiscation		3	Money laundering crime	R.1&R.2
		4	Confiscation and temporary measures	R.3
Terrorist Financing and Proliferation Financing		5	Terrorist financing crime	SR.II
		6	Targeted financial sanction on terrorism and terrorist financing	SR.III
		7	Targeted financial sanction on proliferation financing	New recommendation
		8	Non-profit organization	SR.VIII
Preventive Measures in the Private Sector		9	Financial institution secrecy laws	R.4
	Customer Due Diligence and Record-Keeping	10	Customer due diligence	R.5
		11	Record keeping	R.10
	Additional Measures for Special Cases	12	Senior official	R.6
		13	Foreign currency transaction bank	R.7
		14	Funds or value transfer service	SR.VI
		15	New technology	R.8
		16	Wire transfer	SR.VII
	Reliance, Control and Financial Group	17	Reliance on a third party	R.9
		18	Internal control, overseas branch and subsidiary	R.15&R.22
		19	High-risk countries	R.21
	Suspicious Transaction Report	20	Suspicious transaction report	R.13&SR.IV
		21	Information disclosure and secrecy	R.14
	Designated Non-Financial Businesses and Professions	22	Designated Non-Financial Businesses and Professions (DNFBPs): Customer Due Diligence	R.12
		23	Designated Non-Financial Businesses and Professions (DNFBPs): Other measures	R.16

Category	Subcategory	No.	Recommendations	Second Revision Reference
Transparency of Legal Person and Legal Relation and Beneficial Ownership		24	Transparency of legal persons and beneficial ownership	R.33
		25	Transparency of legal relation and beneficial ownership	R.34
Competent Authority's Power, Responsibility and Institutional and Other measures	Regulation and supervision	26	Regulation and supervision on financial institutions	R.23
		27	The authority of supervisors	R.29
		28	Regulation and supervision on Designated Non-Financial Businesses and Professions (DNFBPs)	R.24
	Operation and Law enforcement	29	FIUs	R.26
		30	Responsibility of law enforcement agencies and investigative authorities	R.27
		31	Power of law enforcement agencies and investigative authorities	R.28
		32	Management of cash couriers	SR.IX
	General Requirements	33	Statistics	R.32
		34	Guidelines and Feedback	R.25
		35	Sanctions	R.17
International Cooperation		36	Implementation of international convention	R.35&SR.I
		37	International cooperation between judicial authorities	R.36&SR.V
		38	International cooperation between judicial authorities : freezing and confiscation	R.38
		39	Extraction	R.39
		40	Other mutual assistance	R.40

* R: Recommendations, ** SR: Special Recommendations

Source: Financial Action Task Force on Money Laundering

1.3.2. Egmont Group

As part of the effort to fight money laundering, governments have created financial intelligence units (FIUs). A number of FIUs have begun working together since 1995. In June 1995, the Egmont Group of Financial Intelligence Units (Egmont Group) was formed at the

FIU plenary meeting organized by the United States and Belgium. The purpose of this group is to the strengthen relationships among FIUs around the globe, support new establishment of FIUs, and enhance cooperation with international organizations to counter money laundering.

To be a member of the Egmont Group, a country's FIU must meet certain requirements. The requirements include: ① adopting the suspicious transaction report (STR); ② establishing the financial information reporting system in accordance with national laws and regulations; and ③ creating an agency to analyze financial information on money laundering. Membership of the Egmont Group is currently comprised of 127 jurisdictions as of August 2011. Korea became a member of the Egmont Group in June 2002.

The missions of the Egmont Group include promoting the establishment of FIUs, encouraging the exchange of information, fostering better communication among FIUs through the Egmont Secure Web (ESW), enhancing training programs·workshops·personnel exchanges, expanding working groups, and developing an appropriate form for sharing information. In order to accomplish its missions, the Egmont Group created five working groups including Training Working Group, Communications Working Group, Legal Working Group, Outreach Working Group, and Operational Working Group. In addition, the Egmont Group Committee, which was established in June 2002, serves as a consultant and coordinator for five working groups and prepares for the annual plenary session.

Korea held the Egmont Group's 16th plenary session for the first time in Asia at the Intercontinental Hotel in Seoul in May 2008.

1.3.3. Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an organization to promote the fight against money laundering in the Asia/Pacific region. In conjunction with the Commonwealth Secretariat, the FATF began the 'Awareness Raising' program in the Asia/Pacific region in 1993. In an effort to implement the FATF's 40 Recommendations, the FATF Asia Secretariat was established in 1995. Its primary objective was to urge the Asia/Pacific region to implement anti-money laundering policies and initiatives and encourage the establishment of an AML regime.

The APG was officially established at the Asia/Pacific Money Laundering Symposium in Bangkok, Thailand in February 1997 and 13 countries agreed to become members of the APG. Located in Sydney, Australia in February 1997, the APG was established and its membership was composed of 16 countries including Korea, Fiji, and India. The primary mission was to provide comprehensive solutions to global money laundering problems at the regional level.

The purpose of the APG is to promote the adoption and implementation of international AML standards in accordance with the FATF's 40 Recommendations, which include suspicious transaction reporting and investigations, establishing FIUs, and enacting legislation on mutual legal assistance·confiscation·extradition·criminal proceedings.

The main activities of the APG include raising awareness of the nature, scope and implications of money laundering, having an agreement to take comprehensive measures against money laundering, implementing overall countermeasures in accordance with the APG, and conducting regular reviews on measures, standards and compliance status.

As of 2012, the APG consisted of 41 members, 5 observer jurisdictions, and 24 observer organizations. The detailed list is as shown in <Table 1-5>.

Table 1-5 | The APG Membership

Division	Number of Country/ Organization	Contents
Members	41	Nauru, Nepal, New Zealand, Niue, Chinese Taipei, Timor Leste, Lao People's Democratic Republic, The Marshall Islands, Macao, Malaysia, Maldives, Mongolia, Myanmar, United States of America, Vanuatu, Bangladesh, Vietnam, Bhutan, Brunei Darussalam, Samoa, Solomon Islands, Sri Lanka, Singapore, Afghanistan, India, Indonesia, Japan, China, Thailand, Cambodia, Canada, Cook Islands, Tonga, Pakistan, Papua New Guinea, Palau, Fiji, The Philippines, South Korea, Australia, Hong Kong
Observer Country	5	Germany, Russia, Micronesia, United Kingdom, France
Observer Organization	24	APEC (Asia Pacific Economic Cooperation), ADB (Asian Development Bank), ADB/OECD Anti-Corruption Initiative, ASEAN (Association of Southeast Asian Nations), CFATF (Caribbean Financial Action Task Force), Commonwealth Secretariat, EAG (Eurasian group on combating money laundering and financing of terrorism), Egmont Group, ESAAMLG (Eastern and South African Anti Money Laundering Group), FATF (Financial Action Task Force on Money Laundering), GAFISUD (Financial Action Task Force on Money Laundering in South America), GIABA (Inter-Governmental Action Group against Money Laundering in West Africa), GIFCS (Group of International Finance Centre Supervisors), IMF (International Monetary Fund), Interpol, MENAFATF (Middle East and North African Financial Action Task Force), MONEYVAL (Council of Europe, Anti-Money Laundering Group), OCO (Oceania Customs Organization), PIFS (Pacific Islands Forum Secretariat), PFTAC (Pacific Financial Technical Assistance Centre), United Nations, UNODC (United Nations Office on Drugs and Crime), World Bank, WCO (World Customs Organization)
Total	70	

Source: Korea Financial Intelligence Unit

1.3.4. Other International Organizations' Main Activities

a. Main Activities of IMF/World Bank

The International Monetary Fund (IMF) and the World Bank (Bank) jointly developed a comprehensive and integrated assessment methodology by including an AML framework when member countries prepare the Financial Sector Assessment Program (FSAP), which assesses the vulnerability of the country's financial sector. The Bank and IMF, in consultation with the FATF, endorsed the comprehensive and integrated assessment methodology at the plenary meetings in 2004, and provided strong consistency by incorporating the FATF's mutual evaluation into the IMF's FSAP.

The three categories of AML/CFT assessment include prudentially regulated sectors like banks stockbrokers and insurance companies, non-prudentially regulated sectors such as bureau de change and trust companies, and the law enforcement sector. The assessment consists of regulations, competent authorizations, and the effectiveness of implementation of regulation. The assessment standards are comprised of judicial proceedings, international cooperation sector, and preventive measures for financial institutions. The details are as shown in <Table 1-6>.

Table 1-6 | AML/CFT Assessment Standards

Judicial Proceedings and International Cooperation	Preventive Measures for Financial Institutions
• Criminalizing money laundering and terrorist financing • Confiscating criminal proceeds and assets for financing terrorism • Providing information on domestically and internationally collected and analyzed by FIU and collection, analysis and dissemination of information on domestic and international basis • The authority and responsibility of law enforcement agencies and prosecutors • International Cooperation	• Customer Identification • Monitoring of accounts and transactions • Record-keeping • Suspicious transaction report • Internal control, compliance with laws and regulations, and audits • Prudential Standards • Cooperation between supervisory authorities and other competent authorities

Source: Financial Action Task Force on Money Laundering

b. Main Activities of the United Nations (UN)

The United Nations (UN) ratified the Vienna Convention in November 1988 to provide provisions for criminal penalties, including the criminalization of drug-related money laundering and confiscation, extradition, and mutual legal assistance. In addition, in June 1998, the UN declared its *Political Declaration and Action Plan Against Money Laundering* to urge countries to take actions on ① identification, freezing, seizure and confiscation of the proceeds of crime; ② international cooperation and legal assistance; ③ verifying the identity of customers and financial record-keeping; and ④ reporting suspicious transactions.

In the wake of the events on September 11, 2001, the UN played a leading role in fostering intergovernmental cooperation by freezing financial assets of both individuals and groups related to terrorism. On September 28, 2001, the UN Security Council adopted Resolution 1373 dealing with the prevention and suppression of terrorist acts. This resolution obligates UN member countries to prohibit assistance to terrorists and freeze assets involved in terrorist acts. The UN Security Council's Resolution 1373 consists of the suppression of terrorists financing and international conventions on terrorism.

1) Main Contents of the Suppression of Terrorist Financing

① Suppressing and preventing the financing of terrorists

② Criminalizing all forms of support for funds directly or indirectly involved in terrorism

③ Freezing financial assets and economic sources involved in terrorist acts

④ Denying the provision of safe haven or support for terrorists

⑤ Criminalizing all forms of acts involved in terrorism, including the financing, planning, and implementation of terrorism, and determining the level of punishment based on the seriousness of terrorist acts

2) Main Contents of International Conventions on Terrorism

① Urging the implementation of all international conventions on terrorism including the *UN Convention for the Suppression of the Financing of Terrorism*.

② Calling for the prevention of the abuse of refugee status by not recognizing terrorists as refugees for political reasons.

1.4. Adoption of Anti-money Laundering System in Developed Countries

The following is the adoption of the AML system in developed countries such as the United States, United Kingdom, Germany, Australia and Japan:

1.4.1. The United States

The United States enacted the Bank Secrecy Act (BSA) in 1970 and the Money Laundering Control Act (MLCA) in 1986 at the federal level with numerous federal or state laws at the federal and state levels.

a. The Bank Secrecy Act (BSA)

The Bank Secrecy Act (BSA) is a typical anti-money laundering law, which provides law enforcement agencies with effective means for crime, tax evasion and financial supervision. The BSA was initially applied to banks, securities firms, bureau de change and casinos. In response to the events of September 11, 2001, the BSA was extended to apply to stockbrokers/dealers, credit companies, mutual funds, and remittance/transfer services. The BSA includes Customer Identification Program & Recordkeeping, Suspicious Activity Reporting , and the implementation of AML program in financial institutions.

1) Customer Identification & Recordkeeping

The Customer Identification (CI) requires financial institutions to verify the identity of each customer when opening an account. In principle, if there are cash transactions in excess of $10,000, the CI requires financial institutions to identify each customer. Customer identification data should be kept for five years. In addition, records for customers' information are required when there are currency instruments such as official bank checks, promissory notes, cashier's checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. Additionally, banks are required to keep records of transfer of more than $3,000, which should include the origin, destination or beneficiary of funds being transferred.

2) Reporting Requirements

Reporting systems include Suspicious Activity Report (SAR), Currency Transaction Report (CTR), Report of International Transportation of Currency or Monetary Instruments (CMIR), and Report of Foreign Bank and Financial Accounts (FBAR). Suspicious Activity Report (SAR) requires financial institutions to report suspicious transactions exceeding $5,000 to the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury. Currency and Monetary Instrument Report (CMIR) requires banks to file a report of CMIR for each shipment of currency or other monetary instruments in excess of $10,000 out of or into the United States with the Bureau of Customs and Border Protection. Currency Transaction Report (CTR) requires banks to report currency transactions above $10,000 to the Internal Revenue Service (IRS). Foreign Bank and Financial Accounts Report (FBAR) requires banks to file the FBAR form to the Department of the Treasury if the aggregate value of financial accounts in a foreign country exceeds $10,000. In addition, financial institutions should carry out internal AML programs, including the appointment of the suspicious activity report officer, the function of independent inspection, and training programs for employees.

b. Money Laundering Control Act

Under the President's Commission on Organized Crime in 1984, the Money Laundering Control Act was enacted as part of reinforcing the criminalization of money laundering and the Currency Transaction Report (CTR) stipulated in the Bank Secrecy Act. The Money Laundering Control Act has a direct influence on the Vienna Convention (1988) and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime adopted by the Council of Europe (1990), having a significant meaning for serving as a model for anti-money laundering.

1) Money Laundering Crime

Under the *Money Laundering Control Act,* money laundering constitutes of two types of crimes: Monetary Instrument Laundering Crime and Monetary Transactions Crime. Monetary Instrument Laundering Crime is divided into money laundering through domestic economic transactions and money laundering through international transportation. On the one hand, money laundering through domestic economic transactions is a financial transaction involving the proceeds of specified unlawful activity that is conducted knowing that the transaction is designed to promote the carrying of specified unlawful activity, or with the intent to avoid tax, or conceal the nature, the location, the source, the ownership, or to avoid a transaction reporting requirement. On the other hand, money laundering through international transportation is an act in which whoever transports, transmits, or transfers a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States, with the intent to promote the carrying of specified unlawful activity, or knowing that the monetary instrument involved in the transportation represent the proceeds of specified unlawful activity and know that the transportation is designed to conceal the source or to avoid a transaction reporting requirement. Monetary Instruments Laundering Crime shall be sentenced to a fine of no more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for no more than twenty years. Meanwhile, Monetary Transactions Crime derives from specified unlawful activity and involves monetary transactions in excess of $10,000. In addition, the Act defines as predicate offences 200 "specified unlawful activity," such as murder, kidnapping, gambling, destruction of property by means of explosive or fire, robbery, racketeering, bribery, fraud, counterfeiting, smuggling, drug trafficking, terrorism, and intellectual property rights infringement.

2) Forfeiture and Retention of Criminal Proceeds

The purpose of asset forfeiture is to take the proceeds out of crime by helping eliminate the ability of the offender to command resources necessary to continue illegal activities and secure public safety. There are two types of asset forfeiture in the United States: Civil Forfeiture and Criminal Forfeiture. Civil forfeiture is a practice that is carried out by means of civil actions or administrative measures *in rem* against laws regardless of criminal procedures; on the other hand, criminal forfeiture is an *in personam* action that is directed at the defendant having a criminal conviction in a civil forfeiture case. In other words, criminal forfeiture is *in personam* actions filed in conjunction with criminal charges. The purpose of civil forfeiture is to forfeit the actual property derived from or used to commit the offense and to eliminate the proceeds from illegal activities so that it can be a separate civil action *in rem* against the property itself derived from or being used to commit a crime. The fundamental aim of criminal forfeiture is to forfeit illegal proceeds as part of the sentence in a criminal case. Criminal forfeiture is basically directed against the defendant personally, and the government brings a criminal action against proceeds or assets from criminal activities.

1.4.2. United Kingdom

The Anti-money Laundering Act in the United Kingdom consists of the Monetary Procedures Act and the Criminal Substantial Act. The Monetary Procedures Act stipulates customer identification, recordkeeping and internal reporting procedures of financial institutions, while the Criminal Substantial Act states the punishment for money laundering and the forfeiture of criminal proceeds. The Monetary Procedures Act contains the *Money Laundering Regulations* enacted in 1993; the Criminal Substantial Act contains the *Criminal Justice Act* 1993, the *Drug Trafficking Offences Act* 1986 as a substitution law of the *Police and Criminal Evidence Act* 1984, the *Terrorism Act* 2000 as a substitution law of the *Prevention of Terrorism*.

a. Money Laundering Regulations

Enacted in 1991 for the purpose of implementing the Committee of the Council of Europe Directive, the *Money Laundering Regulations* regulate financial institutions to prevent money laundering. Under the regulations, “relevant financial business” is required to comply with anti-money laundering regulations. The scope of “relevant financial business” also applies to the provision of advice on investment by lawyers or accountants because relevant financial business includes the provision of relevant financial services not only limited to banks, securities firms, and insurance companies. Relevant financial business is required to take the following five measures.

① Establish internal procedures necessary to prevent money laundering, such as the appointment of a suspicious activity reporting officer to the National Criminal Intelligence Service (NCIS) in case suspicious activity occurs

② Verify the identity of customers or a counterparty if a business relationship is established, such as opening an account; if there is a one-off transaction amounting to EURO 15,000 or more; if there is a suspicion that a transaction is related to money laundering; if there are reasonable grounds to suspect that the actual transactions exceed EURO 15,000 by distributing transactions less than EURO 15,000; and if there is a suspicion that the transaction is to be carried out on behalf of another person

③ Keep a record of each transaction for five years from the end of the business relationship

④ Carry out internal reporting procedures of the *Money Laundering Regulations* if there is knowledge or suspicion that another person is engaged in money laundering

⑤ Provide all employees with appropriate training in the fight against money laundering. If relevant financial business does not comply with provisions, it can face two years imprisonment and/or a fine.

b. Penalties for Money Laundering

Under the *Criminal Justice Act*, money laundering crime consists of concealing or transferring proceeds of criminal conduct (section 93C), assisting another to retain the benefit of criminal conduct (section 93B), acquisition, possession or use of proceeds of criminal conduct (section 93A). The constitution of a crime contains not only knowing that any property is proceeds of criminal conduct but also knowing or having reasonable grounds to suspect. In addition, a person does not commit an offence if, knowing or having reasonable grounds to suspect that any property is proceeds of criminal conduct, he discloses to a constable such a suspicion; a person commits an offence if he does any act in contravention of the disclosure of information. A person guilty of money laundering offences shall be liable on conviction on indictment, to imprisonment for a term not exceeding fourteen years or a fine; on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum.

c. Forfeiture and Retention of Criminal Proceeds

Like the United States where civil forfeiture is applied, the United Kingdom accepts civil forfeiture. Offences applicable to the confiscation of proceeds of criminal conduct are the same as predicate offences of money laundering. In respect of the retention of proceeds of criminal conduct, the High Court shall make a retention order on the request of the prosecutor, make a retention order before the proceedings as well as after the commencement of the proceedings, and cancel a retention order if the court does not institute criminal proceedings for the offence within a reasonable period of time.

2. Korea's AML System and Need for Adoption

2.1. Money Laundering in Korea

2.1.1. Scale of Money Laundering

Ahn Hyun-do and Yoon Chang-in of the Korea Institute for International Economic Policy (KIEP) in 2000, estimated that the scale of money laundering in Korea was roughly KRW 48 trillion to KRW 147 trillion — equivalent to about 11% to 33% of the Gross Domestic Product (GDP). According to the estimate, the enforcement of the second-stage of foreign exchange liberalization in 2001 will allow the cash flows of illegal proceeds to reach about KRW 25 trillion to KRW 50 trillion. Under the circumstances, the Korea Financial Intelligence Unit (KoFIU) was established in 2001 and the *Act on Reporting and Use of Certain Financial Transaction Information* and the *Proceeds of Crime Act* were enacted. In spite of the stringent regulations of money laundering, the amount of money laundering shows no sign of abating.

According to a report published in July 2012 by the Korea Customs Service (KCS), the KCS uncovered foreign exchange activities including foreign currency fraud, where the volume was KRW 2.8 trillion in the first half of the year and accounted for about 83% of 3.4 trillion last year. Moreover, the KCS detected money laundering of KRW 150 billion, up from KRW 120 billion last year. Additionally, the KCS tracked down all illegal foreign transactions such as money laundering, foreign transactions related crime, and refuge assets in the first half of the year totaling about KRW 3.1 trillion.

The KCS detected illegal foreign exchange transaction of KRW 2.3 trillion in 2007, which soared from KRW 3.1 trillion in 2010 to KRW 3.8 trillion in 2011, an increase of 61.3% in 4 years. As the KCS uncovered illegal foreign exchange transactions of KRW 3 trillion, it was estimated to reach a record high of more than KRW 5 trillion in the first half of the year.

2.1.2. Characteristics of Money Laundering

a. Creation of Slush Fund by Corporation

In Korea, economic crimes such as embezzlement and breach of trust take up the largest share of the predicate offences of money laundering, and the creation of slush funds by corporations and the resulting bribery and the provision of political funds have become a social problem. As slush funds are secretly created by companies for the purpose of personal accumulation of wealth, bribery, lobbying funds and entertainment expenses, it takes on a temporary illegal fund depending on the usage.

In most cases, the usage of slush funds is not disclosed. However, it turns out that slush funds are generally used for purposes such as graft, lobbying funds, entertainment expenses, and personal accumulation of wealth. The punishment for money laundering associated with slush funds is highly likely to apply to the predicate offences in the level of the actual use of slush funds including bribery and lobbying funds, rather than the retention of slush funds.

b. Creation of Political Funds

For years, there has been speculation that companies in Korea use most of the slush funds to provide illegal political funds. The speculation was proven true as law enforcement agencies launched an investigation into the presidential election campaign funds. According to the judicial investigation, it turned out that companies and political circles used various methods of money laundering such as deposits and withdrawals by cash and purchases of unregistered bonds in order to conceal the source of funds in the process of creating, providing, and using illegal funds.

In general, predicate offences constitute serious anti-social crimes under *the Proceeds of Crime Act*. However, considering Korea's distinct characteristics of illegal political fund contributions, the scope of predicate offences cover a wide range of crimes against the *Political Fund Act* governing the income and expenditure of political funds.

c. Manipulation of Private Money Market

Traditionally, a private financing institution such as a private money lender naturally came and served as intermediaries for firms or individuals who were hardly able to lend money from public financial institutions such as banks. As the private financing institution was closely interwoven with individuals, it had both advantages and disadvantages. Beginning in the 1960s, there was a boom in the black-market for money.

According to a report published in August 2004 in the news magazine *Shin Dong-A*, the so-called "bond laundering" flourished in the private loan market. Bond laundering is a process in which a private money lender buys low-priced bonds from a person who wishes to cash bearer bonds or Certificates of Deposit (CD) and after years, sells them at above face value through a legitimate intermediary such as securities firms. Such a practice was actually found in the previous investigation of the presidential election campaign funds. For example, when a company provided political circles with illegal political funds in the form of unregistered bonds, it supplied bonds with the actual price plus the payment of a coupon paid to a private money lender. This clearly showed that unregistered bonds were actually traded for cash through the private money market.

In general, money laundering through the private loan market differs from a borrowed bank account, a traditional method of using financial institutions. According to competent authorities, private money lenders colluded with employees from bank branches in advance and laundered illegal funds by disguising transactions as legitimate banking transactions, thereby making it possible for the illegal forms of checks even to be laundered through banks.

d. Capital Outflow Overseas

Under *the Financial Traction Reports Act* (FTRA), an offense to disguise and conceal is subject to a suspicious transaction report because assets are disguised or concealed for the purpose of tax avoidance through foreign exchange transactions. In the past, there were many cases of illegal funds outflows through foreign exchange fraud or local corporations. At present, as the rise in domestic assets is sluggish, there are increasingly cases of investments in overseas real estate in an expedient manner through overseas remittance. In response to illegal activities, KoFIU and relevant law enforcement agencies enhanced efforts to prevent illegal funds outflows made through overseas remittances.

In particular, Korea has seen an increasing volume of offshore hidden assets through tax shelters: the legitimate amount of investments in tax havens alone amount to a whopping KRW 24 trillion; the number of paper companies in tax shelters by local firms approached 5,000. As of 2012, the KCS found that the cases of transferring assets overseas and money laundering increased ten times in four years.

There is a growing danger of crime resulting from capital outflows overseas, as shown in James Henry's report, a former chief economist of McKinsey & Company, that from 1970 through 2010, Korea ranked third in terms of offshore wealth transfers of KRW 888 trillion (about $770 billion).

2.2. The Background and Need for Anti-Money Laundering System

2.2.1. Background of AML System

In today's global economic condition, the economy of one country is inextricably linked to another in various ways. The wave of liberalization in several sectors including trade, financing, and capital led by major developed countries from the 1970s gained momentum spurred by the breakneck development of information technology after the 1980s. Liberalization expanded to agriculture, finance, medicine, and education, resulting in a rapid increase in scale and frequency of capital flows compared to the past.

Using the rapid capital flows, organized crime reaps huge proceeds from money laundering and tax evasion, and the sources of gains are sophisticatedly concealed.

a. Need for AML Regime at the Global Cooperation Level

As part of the efforts to fight money laundering, governments have taken regulatory measures. Because today money laundering is practiced worldwide, there is growing recognition of the need for global efforts through international cooperation rather than individual ones.

Therefore, international organizations related to anti-money laundering strongly urge governments to comply with the AML regime and impose sanctions on non-cooperative countries and territories (NCCT) by terminating intergovernmental financial transactions.

b. Need for AML Regime at the Domestic and International Level

In order to detect and stem the flow of illegal funds associated with drugs, smuggling, and organized crime, developed countries like the United States and international organizations such as the UN and the FATF have recommended that each country establish its financial intelligence unit (FIU) and adopt AML standards. In addition, they impose sanctions on non-cooperative countries by preventing financial transactions.

In Korea, since 2001, illegal fund flows have sharply increased on a cross-border basis, driven by the persistent liberalization of exchange controls. Regarding the changes, there has been the need for establishing an institutional framework to protect financial institutions and the system from being used as an avenue for making criminal proceeds legitimate and to prevent Korea from becoming an international money-laundering platform.

2.2.2. Need for Anti-Money Laundering System

Anti-money laundering system is needed for three objectives: identifying evolving money laundering patterns; enhancing economic transparency and international credit status; and improving financial institutions' credibility.

a. Identifying Evolving Money Laundering Patterns

With the liberalization of foreign exchange transactions across the world, the globalization of financial institutions, and the spread of electronic financial services, the pattern of money laundering has been evolving in various forms. Typical patterns of money laundering include tax shelters or under-regulated countries having no anti-money laundering legislation, non-bank financial institutions, advanced technology and professional brokers due to rising financial gain of criminal organizations, or tax evasion and overseas capital outflows unrelated to drugs.

In addition, as criminal organizations increasingly obtain financial ability, the techniques of money laundering has grown sophisticated using advanced technology and financial experts. Organized crime have taken over financial institutions and enjoy a more cozy relationship with political parties. Using diverse financing techniques such as electronic financial services, organized crime co-mingles the illicit funds with legitimate funds and diverts them across the globe in order to avoid law enforcement.

b. Enhancing Economic Transparency and International Credit Status

By providing strict regulations of criminal proceeds, the AML framework deprives the economic motivation to commit a crime, prevents organized crime from operating illegal proceeds and committing criminal activities, and prohibits investment of illegal proceeds in legitimate business activity from having significant economic and social consequences for countries. Moreover, as the liberalization of foreign exchange transactions makes it easier to transfer funds internationally and to encourage the free flows of illegal proceeds, Korea needs to establish the AML framework in accordance with the international standards in order to avoid being used as a ML platform and play a leading role in Northeast Asia as a financial hub.

c. Improving Financial Institutions' Credibility

Anti-money laundering framework deters financial fraud and bad loans, and to a larger extent enhances the competitiveness of financial institutions since it is viewed as an investment rather than a cost. Furthermore, to deal with international financial instruments due to financial activities at the international level, financial institutions need to improve the international credibility for anti-money laundering in a way that avoids risking their reputations when financial institutions become involved in illegal funds.

Specifically, in September 2005, the United States detected Banco Delta Asia (BDA) based in Macao as a money-laundering platform. In this process, the United States called for financial institutions to cease doing business with the BDA and informed other countries of the oversight of the BDA's illegal financial activity. Accordingly, this damaged the BDA's reputation. Other examples are Asia Wealth Bank and Myanmar Mayflower Bank, of which in March 2005, the Myanmar government canceled the license of banking operations when the United States raised suspicion on drug-related ML activities.

3. AML System Adoption Process

3.1. AML System Adoption Process

3.1.1. Legislation Preparation Stage

After the inauguration of a civilian government in February 1993, Korea launched inspections on public officials in an attempt to create a clean government. Meanwhile, tax-related corruption occurred at a local district in Incheon in September 1994. The scandal paved the way for establishing a fundamental solution to anti-corruption and on January 5 1995, the *Act on Special Cases concerning Forfeiture for Offences by Public Officials* was enacted, which focused solely on the forfeiture of ill-gotten proceeds but failed to contain the punishment provision for money laundering.

After the *Presidential Financial and Economic Emergency Order on Real Name Financial Transactions and Guarantee of Secrecy* was enacted on August 12, 1993, there was growing recognition of an underground economy and money laundering. This led to the adoption of the AML framework coupled with the scandal of a slush fund involving the former president in 1994. Accordingly, the then opposition Democratic Party submitted the *Legislative Bill on Money Laundering Regulation* to the National Assembly on December 7, 1994, but it failed to come into effect in fear of deteriorating the economy.

In December 1995, the *Act on Special Cases Concerning the Prevention of Illegal Trafficking of Narcotics, etc*. was enacted. The purpose of this act was to take a strong countermeasure for narcotic-related crimes, which were a serious social problem both domestically and internationally, and to sign the *UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. This led to the establishment of a regulatory and punitive framework for the predicate offense of money laundering associated with drug crimes.

In July 1997, under the complementary policy of the real-name financial transaction system, the then Ministry of Finance-Economy submitted the *Legislative Bill on Real Name Financial Transactions and Guarantee of Secrecy (Real Name Financial Tractions Act)* and *Legislative Bill on Anti-money Laundering* to the National Assembly. Among them, the Real Name Financial Transactions Act alone was passed in December 1997 and the *Legislative Bill on Anti-money Laundering* was abolished without any deliberation.

The *Act on Special Cases Concerning the Prevention of illegal Trafficking in Narcotics, etc*, which is the only law concerning money laundering, stipulated that money laundering related to drug trafficking alone shall be the component of crime. This led to the difficulty of punishing money laundering offences associated with other serious crimes, such as terrorism, trafficking, and organized crime. Furthermore, it failed to meet international AML standards, such as the poor reporting performance, since it did not take into account the establishment of the STR reporting system and FIU, the authority that analyzes the data.

a. Enactment of the Real Name Financial Transactions Act

The *Presidential Financial and Economic Emergency Order on Real Name Financial Transactions and Guarantee of Secrecy* took effect in August 1993. This paved the way for the practice of identifying and verifying the beneficial owners, which is the most important task for the Customer Due Diligence (CDD), before Korea formally adopted the AML regime in 2001. Furthermore, unlike foreign countries, Korea implemented the Act in advance, so it effectively established the AML framework.

① Adoption Process of the Real Name Financial Transactions Act

In the 1960s, Korea allowed financial transactions under non-real names for the better provision of investment sources in the process of rapid growth. The *Act on Guarantee of Secrecy of Deposits · Installment Deposits* enacted in 1961 stipulated non-real name financial transactions. The act was to facilitate funds in the financial sector at a time when domestic savings were low. As a result, however, negative consequences included: expanding a secret underground economy and abusing financial transactions as a way for tax evasion. In 1982, the scale of the underground economy experienced extraordinary growth. For instance, the volume of the private lending market exceeded KRW 1.1 trillion, representing 7% of the total amount of money (M2). In May 1982, the loan scandal of a husband and wife moneylending team (Lee Chol-hi and Chang Yong-ja) prompted Korea to discuss whether it adopted real name financial transactions system to fulfill social justice through legalization of the underground economy and improving the fairness of the tax burden. As there was a general consensus about the need for the system, the Korean government announced in July 1982 the implementation of the system and a comprehensive income tax system. In December 1982, the *Real Name Financial Transactions Act* was enacted. However, the implementation of the Act was deferred as a result of delegating authority to the government, under which related provisions pertinent to the duty of real name financial transactions among the Act were enforced at a period after January 1, 1986 set out by a Presidential Decree.

In 1982, the rate of real name financial transactions was only 60%, which was deeply rooted in the practice of non-real name financial transactions, and there were many loopholes in both the computing system and tax process in dealing with the Act. Moreover, as the economic situation worsened with the second oil crisis and the massive balance of payments deficits, the resulting side effects occurred: overseas capital flight, capital withdrawals from the banking sector, widespread speculation in currency, and difficulties in financing of businesses arising from the slump in the stock market. The poor response to the problems, ultimately, led to a delay in implementation. After that, the Korean government took measures for promoting the Act. Starting from July 1983, it phased in differential tax rates on financial assets under non-real names and increased the withholding tax rates for income tax from 22.6% in 1983 to 64.5% in 1991. In addition, it made an all-out effort to promote real name financial transactions by producing and expanding financial instruments that should be transacted under real names. It facilitated the conduct of financial transactions under real names by providing comprehensive household deposits, savings deposits, and tax-favored deposits. Furthermore, it continued to carry out projects for providing computing competency between financial institutions and tax administration.

In 1987, the real-name financial transaction system deferred in 1982 resurfaced when presidential candidates incorporated it into their campaign promises. In October 1988, the Korean government announced the implementation through the “Plan for Stable Economic Growth and Advanced· Balanced Economy” starting from January 1991. It promoted the enforcement of the system that caused public controversies between 1989 and at the beginning of 1990. In April 1989, it launched the ‘Task Force for Real-Name Financial Transaction System’ within the Ministry of Finance and established ‘the Committee for Real-Name Financial Transaction System’ tasking government departments and heads of financial institutions to come up with feasible measures to improve the system and come up with solutions to possible side effects. However, after the second half of 1989, as concerns of an economic crisis came to the fore, due to sluggish economic growth, aggravated balance of payments deficits, a slump in the stock market, and possible speculation in real estate, the implementation was deferred after a series of exhausting debates. The real-name financial transaction system, which had been at the center of controversy for a decade, was finally enforced on August 12, 1993 at 20:00 pm under the presidential emergency order. In 1992, during the presidential election, candidates vowed to implement the system that was announced by the presidential emergency order. Under the order, the existing *Act on Real Name Financial Transactions and Guarantee of Secrecy* was abolished and everyone was required to use their real names when they conducted financial transactions with financial institutions.

② Main Enforcement

The *Presidential Financial and Economic Emergency Order on Real Name Financial Transactions and Guarantee of Secrecy* largely falls under the following three categories: stipulating the use of real names when conducting transactions with financial institutions; stating measures for the existing non-real name assets; and strengthening the guarantee of secrecy of financial transactions.

First, a legal entity or an individual shall conduct all financial transactions with financial institutions under real names.

Financial institutions ranging from banks, security finance companies, insurers, a trust business entity to local unions including agricultural cooperatives, post offices, and community credit cooperatives, shall perform financial transactions with customers under their real names. The Act requires the individuals to enter his or her real name in a resident registration card, and the legal entity to enter its business registration certificate. Officers and employees of financial institutions shall face a fine in violation of such provisions.

Second, with respect to assets transacted under non-real names, the Act prevents withdrawals of all assets before the identification of real names.

The Act prevents assets from being held under non-real names or in cases where the legal entity or the individual fails to identify his or her real name. In addition, after a certain grace period after the enactment of this Act, assets with non-real names are required to convert their names into real ones. Accordingly, the identified income shall be subject to taxation. A person shall face harsh penal provisions in violation of the Act.

Third, to alleviate the risk of disclosed information from the provision of transaction information, the Act requires a guarantee of secrecy of financial transactions.

Under the Act, no person working for financial institutions shall provide information on financial transactions to other persons unless he receives a request or consent in writing from the holder of a title deed. To strengthen the role of the guarantee of secrecy, the same shall apply to any of the following cases in which the transaction information is requested or provided to the minimum limit necessary for the purpose of use thereof:

Provision of transaction information by a court order to produce, or by a warrant issued by a judge; Provision of tax data which must be submitted under tax-related Acts; Provision of transaction information necessary to supervise and inspect financial institutions; Provision of transaction information necessary for business inside any financial institution or between financial institutions; and other provision of any transaction information under Acts which must be disclosed to various persons under the relevant Acts.

However, in the event that anyone requests the provisions of transaction information, transaction information is requested or provided by means of the standard form to the minimum limit necessary for the purpose of use. Where persons working for financial institutions receive a request for the provision of transaction information in violation of the articles, they shall refuse it. With the provision, information leakage from the abuse of law is prevented. In addition, a person who violates the provisions shall be punished under harsh penal provisions.

3.1.2. System Adoption Stage

a. Background of Legislation on Anti-money Laundering

As the UN urged each country to enforce the AML framework in place, Korea needed to participate in the global effort to combat money laundering. In response, Korea established the International Financial Intelligence Unit Task Force (FIU TF team) in the Ministry of Finance and Economy in April 2000 and promoted the AML system. In particular, as the second stage of foreign exchange liberalization took effect from January 2001, Korea needed an institutional framework to monitor the flow of illegal funds from the misuse of financial liberalization. And this was one of the main reasons to accelerate the adoption of the AML system.

What was commonly known as *Legislation on Anti-money laundering* was divided into the *Proceeds of Crime Act* under the Ministry of Justice and into the *Act on Report on, and the Use of Specific Financial Transaction Information* (the *Financial Traction Reports Act* (FTRA)) under the Ministry of Finance and Economy.

During the discussion at the National Assembly's Legislation and Judiciary Committee, there was a delay in considering legislation to determine whether predicate offences should cover an offense committing the *Political Fund Act*. The several focal points included: ① adopting a notification system to report and analyze in case of political fund offences; and ② taking countermeasures for the abuse of the right to track account records by an FIU without warrant.

On April 23, 2001, during discussions of the nine member committee, which consisted of floor leaders from three political parties, assistant administrator on the Finance and Economy Committee and the Legislation and Judiciary Committee, there were agreements on two cases: ① in case of Customer Due Diligence of political fund offences, suspicious transaction information in the hands of an FIU is passed to the National Election Commission so while the person is under a general investigation into the political fund, the person gains the opportunity to give the committee proper explanations; and ② deleting FIU's right to track account records without warrant. After the ongoing discussions on the right to track account records by a FIU, the legislation was ultimately passed by vote.

This provided an avenue to punish illegal money laundering activities, under which the reporting·analyzing·provision system regarding suspicious transactions was established to take preventive measures.

b. Enactment of the Financial Traction Reports Act (FTRA)

In most cases, money laundering is carried out through financial institutions. Therefore, the systematic collection and analysis of information on money laundering are important in effectively preventing money laundering. As a result, the *Financial Traction Reports Act*

(FTRA) put an emphasis on preventing financial institutions from being used as money laundering platforms and on providing law enforcement with information in relation to money laundering during an investigation process.

After the FTRA was enacted in November 2011, Suspicious Transaction Report (STR), Currency Transaction Report (CTR), and Customer Due Diligence (CDD) followed suit, constituting the three main pillars of anti-money laundering.

a) The Enactment (November 2001)

When the *Financial Traction Reports Act* (FTRA) was enacted, the FTRA consisted of ① establishing a Financial Intelligence Unit (FIU); and ② adopting Suspicious Transaction Report (STR).

① Establishing a FIU

The Korea Financial Intelligence Unit (KoFIU), which is under the Ministry of Finance and Economy, independently performs the duties within its own authority. KoFIU's officials shall not be engaged in any other activities than specified in this Act. The independence of KoFIU was guaranteed by law; the organization and operation of KoFIU shall be determined by Presidential Decree in consideration of the independence and political neutrality.

② Adopting Suspicious Transaction Report (STR)

Financial institutions are required to report suspicious transactions to KoFIU without delay if there are reasonable grounds to suspect that funds are derived from illegal activities; if there is suspicion that funds are linked to money laundering; if there are transactions exceeding a fixed threshold amount set by Presidential Decree. If relevant financial business does not comply with provisions, it can face a fine of up to KRW 5 million.

Furthermore, when the *Financial Traction Reports Act* (FTRA) was enacted, the enforcement ordinance stated that a designated threshold of a suspicious transaction report should be $10,000 in foreign currency and KRW 50 million in local currency. This was designed to minimize the burden of reporting by financial institutions and to adjust the threshold at the same time without making a dent in financial transactions of the public. After the suspicious transaction report (STR) took root without having damaging influence on general financial transactions and at the same time, the STR did not put an onerous burden on financial institutions, the threshold was lowered to KRW 20 million in January 2004.

b) The First Revision (January 2005)

Domestically, with the launch of the participatory government in 2003, there was a growing recognition of the prevention of illegal funds and the transparency of financial transactions. Internationally, after the events of September 11, 2001, there were concerted efforts to strengthen the AML system, as well as efforts to combat the financing of terrorism.

In response to these efforts, both domestically and internationally, Korea promoted the revision of the FTRA that financial institutions should adopt Currency Transaction Report (CTR) and Customer Due Diligence (CDD) to improve an AML system in Korea. Passed in the National Assembly in December 2004, the revised bill was promulgated in January 2005, the first amendment since the enactment. The main contents of the revision are as follows:

① Adopting Currency Transaction Report (CTR)

A Currency Transaction Report (CTR) requires financial institutions to report currency transactions exceeding a designated threshold to KoFIU. While Suspicious Transaction Report (STR) requires financial institutions to report only if there is suspicion that funds are linked to money laundering on a basis of the subjective and specialized judgment of financial institutions, the CTR requires financial institutions to report all transactions in currency of the threshold regardless of whether there is a suspicion that funds are linked to money laundering in accordance with general rules. Thus, the CTR plays a role in complementing STR that is based on the subjective judgment of financial institutions.

In January 2006, when the FTRA was enforced, the threshold and time frame for lowering the amount were stated in addendum of Enforcement Decree of the Act. The threshold was KRW 50 million in 2006, but lowered to KRW 30 million in 2008 and 20 million in 2010, as stated in the addendum.

② Adopting Customer Due Diligence (CDD)

With regard to the identity of customers and the purpose of transactions, Customer Due Diligence (CDD) requires financial institutions to conduct ongoing due diligence in order to ensure that their services did not assist money laundering. Financial institutions in other developed countries have carried out the system called "Know Your Customer."

In Korea, financial institutions were required to verify the identity of each customer under the *Act on Real Name Financial Transactions and Guarantee of Secrecy*. This was, however, not sufficient to comply with the FATF Recommendations. In particular, the CDD, as one of the FATF Recommendations, is required to implement when preparing the Financial Sector Assessment Program (FSAP) by the Bank and IMF in 2003. In response to this, the CDD was adopted by revising the FTRA.

③ Providing Suspicious Transaction Information on Political Funds

Financial institutions were required to report suspicious transaction information violating the *Political Fund Act* only to the National Election Commission. However, under the revision, such a provision was deleted to provide suspicious transactions information on political fund-related money laundering to law enforcement agencies just like predicate offences.

c) Revision of Enforcement Decree (March 2010)

On October 14, 2009, Korea became a member of the FATF and submitted an action plan to improve Korea's Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) regime, complying with the international standards. The action plan included taking action to remedy the deficiencies in mutual evaluations of Korea, which was adopted in the FATE plenary meeting in June 2009. The main objective of the action plan, in the short-term, was to enact AML/CFT regulation for financial institutions to follow and to lower the threshold of suspicious transaction reports. To do this, the Enforcement Decree of the FTRA was amended.

The two main contents of the revision consist of: ① establishing new grounds for regulation; and ② lowering the threshold of suspicious transaction reports.

① Establishing New Grounds for Regulation

Under the revised Enforcement Decree of the *Financial Traction Reports Act* (FTRA), the commissioner of KoFIU shall have the authority to notify and determine the necessary requirements for the implementation of AML obligations, such as internal control & reporting regime, customer due diligence, establishment of monitory system, and record-keeping in relation to financial institutions' AML efforts.

In September 2008, KoFIU provided financial institutions with the *AML Enforcement Guidelines* governing the standards for the fight against money laundering. The *AML Enforcement Guidelines* was, however, not legally binding financial institutions and did not include standards for imposing sanctions of non-compliance. Because the *AML Enforcement Guidelines* was not a binding legal obligation, the assessors of mutual evaluations did not recognize the *AML Enforcement Guidelines* as AML framework.

The revision paved the way for establishing a legal framework, thereby enabling the commissioner of KoFIU to substitute the existing *AML Enforcement Guidelines* with the *AML Regulation*. Accordingly, this enabled Korea to establish an AML framework in compliance with the international AML standards and at the same time provided financial institutions with the specific standard for dealing with AML obligations.

② Lowering the STR Threshold

In 2001, as Korea adopted the Suspicious Transaction Report (STR) under the *Financial Traction Reports Act (FTRA)*, Korea decided to gradually lower a designated threshold, which was KRW 50 million, in an attempt to ease the burden of financial institutions and to dispel public anxiety. At the first stage, the threshold was lowered to KRW 20 million in 2004. During mutual evaluations, however, the assessors pointed out that Korea only applied STR to transactions exceeding KRW 20 million. Assessors recommended that Korea should abolish the application of the threshold because the threshold was inconsistent with the international standards and led to the increased risk of money laundering and terrorist financing. In response to this concern, the STR reporting threshold was lowered to KRW 10 million ($50 million) under the *Enforcement Decree of* the *FTRA* since July 2010.

c. Legislating the Proceeds of Crime Act

The purpose of the *Proceeds of Crime Act* is to prevent money laundering and to eliminate the underlying contributing factors of specific crimes by regulating activities that conceal or disguise criminal proceeds related to specific crimes, and prescribing special cases regarding confiscation and collection with regard to criminal proceeds related with specific crimes. The act consists of the definitions of specific crimes, the punishment of money laundering activity, and the extension of confiscation of criminal proceeds and collection.

a) Definition of Specific Crimes

Predicate offences are offences for acquiring illegal proceeds subject to money laundering crime, confiscations, and collection including ① serious crime as prescribed in an attached table under the *Proceeds of Crime Act* and ② offences under subparagraph 2 (b) of this Article.

Serious crime is a crime committed for the purpose of acquiring illegal proceeds. The offences are as follows:

① Offences involving serious crimes such as murder, robbery;

② Offences in which criminal organizations professionally and occasionally commit for the purpose of proceeds of criminal activity and in violation of racketeering, violent actions, sexual exploitation, smuggling, Prevention of Prostitution, etc. Act;

③ Offences which relate to economic activities for the purpose of high proceeds of crime in Article 3 (fraud etc.) of the *Act on the Aggravated Punishment, etc. of Specific Economic Crimes* and in violation of the *Securities and Exchange Act*;

④ Offences involving corruption and in violation of *Bribery Act , Political Fund Act, Attorney-at-Law Act*;

⑤ Offences relating to illegal offshore wealth transfers under foreign exchange market liberalization and import-export price manipulation; and

⑥ Offences which are designated as predicate offenses of money laundering widely adopted by developed countries and forgery of currency documents.

Crimes under subparagraph 2 (b) of this Article are related to organized crime or constitute a highly regulated subject for the purpose of international cooperation and promoting foreign exchange market liberalization as follows:

① Offences involving the provision of funds for the purpose of forming or retaining organizations or groups conducting violent activity under Article 5 (2) of the *Punishment of Violence, etc. Act*;

② Offences related to funding the act of prostitution including providing place or arrangement as prescribed in subparagraph 3 Article 25 (1) of the Prevention of Prostitution, etc. Act;

③ Criminal liability of persons offering bribery under Article 3 (1) of the Act on Combating Bribery of Foreign Public Officials in International Business Transactions; and

④ Crime of property moving to foreign country under Article 4 of the Act on the Aggravated Punishment, etc. of Specific Economic Crimes.

b) Punishment of Money Laundering

A person shall be sentenced to a fine of less than KRW 30 million or imprisonment for less than five years if he disguises the acquisition, disposition, or origin of criminal proceeds and if he conceals the criminal proceeds by purpose to encourage specific crime or to disguise criminal proceeds as legitimately acquired.

A person shall be sentenced to a fine of less than KRW 10 million or imprisonment for less than two years if he attempts to conduct the disguising and concealing of criminal proceeds; if he prepares or conspires for the purpose of concealing or disguising criminal proceeds.

c) Confiscation · Collection of Criminal Proceeds

The *Proceeds of Crime Act* broadened a wider scope of the target for confiscation beyond the Article 48 of the Criminal Code. In other words, under Article 48 of the Criminal Code, confiscation is only applicable to property. However, under the *Proceeds of Crime Act*, confiscation shall be applicable to all profits that generate sociologically economic value including intangible profits such as bank deposits, loan, and intangible property rights. In addition, the Act stated that confiscation shall be applicable to assets if the assets from a specified crime can be transferred or transformed.

Under the *Act on Special Cases concerning the Prevention of Illegal Trafficking in Narcotics, tec.* or the *Act on Special Cases concerning Forfeiture for Offences by Public Officials*, compulsory confiscation shall be adopted for the purpose of the forfeiture of proceeds. However, arbitrary confiscation shall be adopted in light of the fact that specific crimes applicable to the *Proceeds of Crime Act* constitute various types of crimes. Accordingly, it is desirable to determine whether the confiscation order is made depending on concrete circumstances.

When it is impossible to confiscate the property under the provisions of Article 8 (1) or when it is deemed to be inappropriate to confiscate the property in light of the nature of such property, the conditions of its use, the existence of a right of any person other than the parties to the offense to such property, or other circumstances, the monetary equivalent to the value of such property may be collected from any parties to the offense.

Meanwhile, confiscation·collection·retention system, which temporarily bans confiscation or collection of assets under investigation or a trial, was adopted for the purpose of effective regulation of the proceeds from crime.

d) Revision of the Act (April 2012)

With a view to including the widest range of offences as money laundering predicate offences, or applying the crime of money laundering to all serious offences, the *Proceeds of Crime Act* was amended in April 2012. The purpose of the revised act is to prevent money laundering by eliminating crime-related proceeds and to a lager extent include the following serious crimes as predicate offences of money laundering if a person conducts wastes management business without license under the *Wastes Control Act*; if a person gets permission by fraud, unlawful means; if a person illegally allows any foreigner who is subject to the immigration checkpoint the *Immigration Control Act* to enter for profit or arranges the acts; and if a person arrange the issuance and reissuance of a passport by unlawful means against the *Passport Act* or he transfers or lends a passport to another person for its use. The revision has a contributing effect on the implementation of Recommendation 3 and 35, Special Recommendation I by including environmental offences (in violation of the *Wastes Control Act*) and criminal acts related to international organized crime (in violation of the *Passport Act* and the *Immigration Control Act*) as the predicate of money laundering. This is part of the legislation for remedying deficiencies raised by the FATF/APG mutual assessment of Korea.

d. Enactment of the Prohibition of Financing for Offences of Public Intimidation Act

a) Enforcement (December 2008)

In order to prohibit the financing of terrorism, Korea enacted the *Prohibition of Financing for Offences of Public Intimidation Act* on December 21, 2007 and enforced this Act on December 22, 2008. The Act is legally binding for implementing the *UN Convention for the Suppression of the Financing of Terrorism* which Korea signed and ratified.

Under this Act, a person shall be sentenced to a fine of less than KRW 100 million or imprisonment for less than ten years if he attempts to raise, supply, or transport funds or assets for the purpose of intimidating the public such as killing a human and injuring a body part. In addition, if any individual or organization is deemed to be related to the financing of terrorism pursuant to subparagraph 1 of Article 4 of this Act, the Financial Services Commission designated the 974 individual or organization as a person or organization whose financial transactions are restricted. This paved the way for the enforcement of the *Prohibition of Financing for Offences of Public Intimidation Act*.

Furthermore, casino operators have complied with the AML/Prohibition Against the Financing of Terrorism framework since December 22, 2008. The FATF Recommendations stipulated that each country should designate lawyers, accountants, casinos, real estate brokers, precious metal dealers, trust and company service provider as non-financial businesses and professions (DNFBPs) and implement the AML/CFT framework for NDFBPs. However, Korea initially implemented an AML framework concerning casinos that were deemed as having high potential for money laundering in local settings.

Casino operators are currently in compliance with Suspicious Transaction Report (STR), Currency Transaction Report (CTR), and Customer Due Diligence (CDD) and have created their own AML internal control guidelines based on the *AML Business Manual* for casinos provided by KoFIU.

b) Revision of the Act (September 2012)

The *Proceeds of Crime Act* covered a wider scope of the target for confiscation beyond the Article 48 of the Criminal Code. In other words, in June 2009, the assessors evaluated that confiscation under Article 48 of the Criminal Code in Korea was far below the international standard, therefore recommending that Korea should improve the CFT framework in accordance with international standards. Considering that Korea became a full member of the FATF and co-chaired the G20 in 2010, the Korean government needed to set the CFT framework to meet the international standard.

The assessors pointed out three deficiencies: ① Korea did not meet the requirements of freezing the terrorist financing set forth in *the UN Convention for the Suppression of the Financing of Terrorism* because it limited the designated person who is restricted from financial transactions only to “financial transactions with financial institutions.”(Special Recommendation III); ② Korea failed to criminalize the financing of terrorist or terror organizations in regard to the criminalization of the financing terrorism (Special Recommendation II); and ③ Korea needed to institute punitive regulations for any person who provides funds to a restricted person.

In order to remedy the deficiencies, the Korean government amended the legislation effective as of September 16, 2012. The main contents are as follows.

① Criminalizing the Financing of a Person Related to Terrorism (natural or legal persons)

In Korea, the *Prohibition of Financing for Offences of Public Intimidation Act* stipulated that any individual or organization shall face punishment only if the individual or organization provides funds for terrorist activities, that is, directly provides funds for terrorist activities. However, the FATF recommends that each country should prohibit the financing of terrorist organization or terrorists, as well as funds related to terrorism.

There are no definitions of terrorist or terrorist organization in the *Prohibition of Financing for Offences of Public Intimidation Act*. In this regard, the scope of punishment included a person who collects and provides funds or assets to a restricted person, who engage in terrorism.

② A Wider Scope of Restriction on Transactions concerning Terrorism

The mutual evaluation teams pointed out that Korea's restriction on the financial transactions system served as mere limitations on financial transactions and failed to perform a freezing mechanism. Furthermore, such a system was only applied to financial assets and failed to cover movable·immovable property.

Under the *Proceeds of Crime Act* enforced on June 19, 2009, confiscation and retention measures can be applicable to funds or assets related to terrorist financing against public intimidation. Thus, confiscation and retention measures for movable·immovable property may serve as a freezing mechanism. However, as the assessors pointed out deficiencies in a freezing mechanism, Korea without delay took action to broaden the scope of the restriction on financial transactions system to include movable·immovable property.

③ Improvement on Granting Permission

Under the *Prohibition of Financing for Offences of Public Intimidation Act*, a designated person who is restricted from financial transactions is required to seek permission from the Financial Services Commission (FSC) if he attempts to conduct financial transactions with financial institutions or make payment or receipt. In addition, if the designated person seeks permission to carry out financial transaction, the person needs to get permission from the FSC.

However, the designated person mostly constitutes a foreigner or foreign entity so the problem occurs when the foreigner or foreign entity should apply for permission to conduct transactions. In light of the problem, Korea broadened the scope of permission to cover the corresponding party other than the designated person, as well as the scope of restriction on transaction regarding terrorism.

④ Deletion of Imposition of Fines Procedure

The *Act on the Regulation of Violations of Public Order* stipulated procedures for the imposition, collection, and execution of and trials on fines for negligence under the supervision of an administrative agency. If the provisions of any other act conflict with those of this act, this act shall prevail. For instance, under the *Prohibition of Financing for Offences of Public Intimidation Act*, any party may raise an objection within 30 days from the date on which he is notified of the imposition of the fine and the court shall bring the case to a trial on fines under the Non-Contentious Case Litigation Procedure Act. On the other hand, under the *Act on the Regulation of Violations of Public Order*, any party may raise an objection within 60 days from the date on which he is notified of the imposition of the fine. In order to correct inconsistency in both laws, some provisions of the *Prohibition of Financing for Offences of Public Intimidation Act* in conflict with the *Act on the Regulation of Violations of Public Order* were deleted. In addition, some provisions of the *Prohibition of Financing for Offences of Public Intimidation Act* regarding judicial proceedings on fines specified in the *Act on the Regulation of Violations of Public Order* were deleted.

e. Establishment and Operation of KoFIU

The Financial Intelligence Unit (FIU) is an agency that is responsible for collecting, analyzing, and disseminating information related to money laundering. If Korea is to institute the AML framework commensurate with the international standard, it should establish a FIU. The main roles of Korea's FIU are as follows:

① Guarantee of Secrecy in Bona Fide Customers

As an intermediary agency between financial institutions and investigation agencies, KoFIU is to act as a buffer between the two conflicts of interest for building confidence, facilitating an efficient STR, and providing reliable information on money laundering with investigation agencies through the analysis of STR. The objective of KoFIU is to serve its purpose by guaranteeing the confidentiality principal for bona fide customers and at the same time combating money laundering.

Under the circumstance, Korea established KoFIU within the Ministry of Finance and Economy, rather than as a law enforcement agency. This enables KoFIU to secure independence of its task and make best use of professionals dispatched from law enforcement agencies by providing a review and analysis of information on financial transactions.

② Systematic and Effective Processing of Money Laundering Information

A FIU, which manages integrated suspicious transaction information filed from financial institutions, conducts the analysis using its specialized experts, thereby bringing about the effective management of money laundering information and transfers the filtering data with suspicious transaction reports to the investigative authority. Accordingly, establishing a FIU can reduce the burden of investigative agencies. In Korea, exceptionally, the right to track account records is confined to overseas transactions so that this can put limitations on the comprehensive analysis on money laundering.

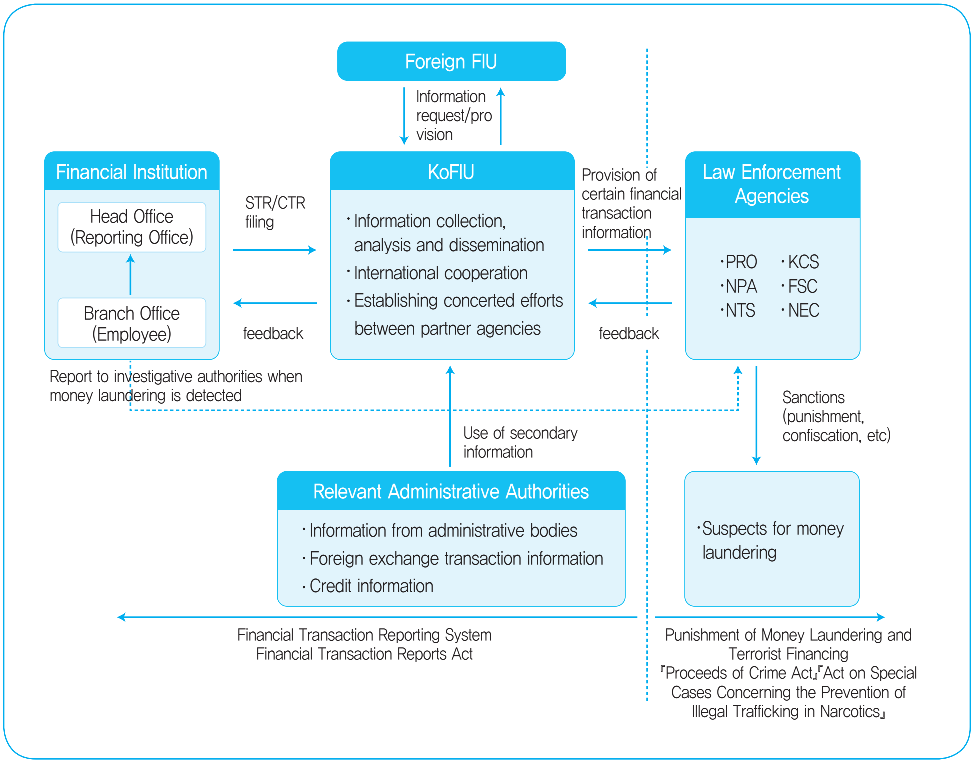
③ Inspection, Training, and Promoting Anti-money Laundering

For the anti-money laundering framework to be effective, financial institutions and the public need to raise the awareness of the importance of an AML framework. To do this, financial institutions should establish a sound practice for financial transactions. Accordingly, the FIU is devoted to supervising AML requirements for financial institutions and providing various training and promotion for raising the awareness of the public as well as financial institutions.

④ Avenue to International Cooperation regarding Money Laundering Crime

In order to effectively cope with the international transfer of illicit funds and the characteristics of money laundering crimes, there is a growing need for international cooperation. Accordingly, each country has a FIU in place to play a part in international cooperation. In the meanwhile, Korea takes part in international efforts by establishing a FIU and is a full member of the APG, the FATF and the Egmont. Moreover, KoFIU enhances bilateral cooperation by contracting MOUs with other countries' FIUs, figures out international trends by actively taking part in international discussion on the fight against money laundering, and serves as an avenue to international AML cooperation for the application of such trends domestically.

Figure 1-1 | AML/Prohibition Against the Financing of Terrorism Framework



Sources: KoFIU

3.1.3. Take-off Stage

Korea became the 35th member of the Financial Action Task Force (FATF) in October 2009, gaining an international reputation for transparent overseas financial transactions. To become a member, a country should undergo the mutual evaluation prepared by the FATF-APG members. There are five steps including: ① submitting mutual evaluation/detailed questionnaire for the implementation of AML/CFT, relevant data on laws and regulations; ② carrying out an on-site visit to the country by the evaluation team; ③ discussing the draft of mutual evaluation reports and submitting countermeasures; ④ finalizing compliance ratings through assessors' meeting; and ⑤ reporting mutual evaluation reports to the Plenary meeting, and preparing & submitting a follow-up report. Among the processes, Korea underwent 1 to 2 steps in 2008 and 3 to 5 in 2009.

The draft on mutual evaluation report of Korea was filed on February 6, 2009. The evaluation report provides a summary of the compliance with the FATF 49 Recommendations and grants the rating of compliance concerning the Recommendations. The rating the FATF-

APG evaluation team granted to the draft of Korea was far below the average of the FATF 20 member countries. This clearly showed how wide the gap was between Korea's own self-assessment and the international mutual evaluation. Most of all, the rating of compliance with the main 14 Recommendations, the criteria for the FATF membership, was far lower.

There were two rounds of opportunities for Korea to supply supporting material after the evaluation team obtained the draft of mutual evaluation of Korea. Making the best use of the opportunity could upgrade a country's rating. Accordingly, the Korean government took active measures to present evidence and persuasive arguments, raised a question about whether the ratings on the draft were inappropriate, and asked for an upgrade of the rating. During this process, the FATF-APG evaluation team held a session to finalize the overall rating for each Recommendation after reviewing the additional explanations for the draft of the evaluation report and the supporting compliance data.

In the evaluation session, Korea received rating upgrades for 12 Recommendations, the largest in history for the FATF mutual evaluation. This was mainly attributed to the provision of a position paper by Korea. Above all, with no specific provision in law in place, Korea was unable to undergo the evaluation for certain Recommendations. Under the circumstances, Korea was able to comply with the implementation of the FATF Recommendations by gathering precedents of the Supreme Court. Most importantly, this was attributable to the close cooperation and active participation between the relevant authorities of the evaluation team, with whom Korea made a good impression.

The FATF/APG mutual evaluation report of Korea was referred to the FATF 20th Plenary at 3th meeting on July 25, 2009, and after a heated debate was officially adopted. The evaluation of Korea was jointly conducted by both the FATF and the Asia/Pacific Group on Money Laundering (APG) so that the results of the evaluation report were also reported to the annual APG meeting in July 2009. Through the discussion of the results, the mutual evaluation report was officially adopted.

However, the results of the mutual evaluation of Korea failed to meet the criteria of the FATF membership. Thus, Korea had to submit a follow-up report for remedying deficiencies identified in the evaluation report to become a full member. This is standard procedure for accepting a member on the condition that a country would take additional steps to address deficiencies, though the results fail to meet the FAFT criteria.

In this regard, Korea submitted the follow-up reports to the FATF on May 2009 and on September 2009. The purpose of the first follow-up report was that the mutual evaluation report was adopted at the FATF Plenary session in June 2009 and at the same time Korea became a full member.

The second follow-up report, which was submitted to the FATF on September 2009 for compliance with AML/CFT frameworks, focused mainly on remedying deficiencies identified in the mutual evaluation report. The second report contained three steps of detailed compliance throughout three years and provided the method of compliance and the revision plan for laws and regulations: short-term tasks completed by December 2009; intermediate-term tasks completed by June 2010; and long-term tasks by June 2012. The second report contained strict measures for effectively improving the AML/CFT regime in Korea, including related law revision and enactment. In addition, measures for deficiencies were prepared based on the discussion and consultation with related authorities such as the Financial Services Commission, the prosecutor, law enforcement, the Ministry of Justice, entrusted inspection agencies and private agencies including financial institutions and casinos.

After the on-site visit to Korea on November 2008, the FATF members at the Plenary in October 2009 assessed that Korea took proper measures for remedying deficiencies in the mutual evaluation report and displayed a firm determination to be well qualified as a full member.

On October 14, 2009, there was the 2nd discussion on whether Korea could become a member of the FATF at the FATF 21st plenary meeting in Paris. The FATF members welcomed Korea as a full member, stressing that Korea, as a co-chair country in the G20, played a key role in the international community. Emphasizing that Korea's entering into the FATF membership brought about the consolidation of AML/CFT regime on a worldwide level as well as the strengthening the FATF, the FATF members called for Korea to cooperate in protecting the international community from money laundering and the financing of terrorism.

In doing so, Korea fully adopted an AML regime in 2001 and succeeded in becoming a full member of the FATF, which was a long-term objective since the establishment of KoFIU. Furthermore, this was a contributing factor for Korea in gaining international recognition.

3.2. The AML System in Korea

In 2005, with the help of the first revision of the FTRA, the three pillars of an existing AML regime were completed: suspicious transaction report (STR), currency transaction report (CTR), and customer due diligence (CDD). The main program is STR. Both CTR and CDD are supporting programs for complementing STR, which is based on the subjective judgment of financial institutions. Currently, an AML regime is applicable only to financial institutions, but it is expected to expand the scope of the application with Korea entering into FATF membership. The AML/CFT operating framework is shown in [Figure 1-2].

Figure 1-2 | AML/CFT Framework

KoFIU	Suspicious Transaction Report (STR)	Currency Transaction Report (CTR)
KoFIU ↕ Financial Institutions	■ Reporting subject · If there are reasonable grounds to suspect that funds are related to money laundering ■ Characteristics · Reporting based on the subjective and specialized judgment of financial institutions · Applicable to all transactions including a transaction in ■ A designated threshold (revised on June 2010) · More than KRW 10 million (in local currency) · More than $5,000 (in foreign currency)	■ Reporting subject · There are transactions exceeding a designated threshold for a business day at the same financial institution by the same person ■ Characteristics · Reporting based on objective and uniform standard · Applicable to only transactions in currency (cash payment · receipt) in financial transactions ■ A designated threshold – KRW 20 million* (except foreign currency) * KRW 20 million starting from 2010

Financial Institutions	Customer Due Diligence (CDD)	
Financial Institutions ↕ Customer	① Verifying the identity of customers ■ Identifying target · Opening a new account · A one–off transaction in excess of KRW 20 million ($10,000) ■ Checklists · Real name, resident registration number, address, contact information	② Identifying customers when there is doubt about money laundering ■ Identifying target · Beneficiary owner is suspicious · Customers are likely to conduct money laundering acts ■ Checklists · Beneficiary owner · The purpose of transaction, etc.

Source: KoFIU

3.2.1. Suspicious Transaction Report (STR)

Suspicious Transaction Report (STR) is one of the major measures for fighting money laundering. If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to money laundering, it should report its suspicions to the applicable financial intelligence unit (FIU).

a. Basic STR Framework

When financial institutions report suspicious transactions to KoFIU, KoFIU collects and analyzes ① suspicious transactions filed and ② foreign exchange transaction information, credit information, and information from foreign FIUs. If the information is deemed as suspicious transactions related to money laundering, KoFIU provides transaction records for law enforcement agencies, including the Public Prosecutors' Office, the National Police

Agency, the National Tax Service, the Korea Customs Service, the Financial Supervisory Commission and the National Election Commission. Accordingly, law enforcement agencies launch investigations into the transactions and prosecutes in accordance with the law.

b. STR Subject

Financial institutions are required to report suspicious transactions to KoFIU ① if there are financial transactions exceeding KRW 20 million ($10,000) and there are reasonable grounds to suspect that funds involve illegal activities or clients are related to money laundering; and ② if they report transactions to investigative agencies after knowing that funds are related to criminal proceeds or money laundering. Any failure to report the STR is subject to punitive measures such as imposing sanctions on related employees and levying a fine on a financial institution. Furthermore, if a suspicious transaction is below the designated threshold, financial institutions have the discretion to report it.

As the reporting threshold was lowered to KRW 20 million from KRW 50 million in January 2004 and there was growing recognition among financial institutions, the cases of suspicious transaction report (STR) have been on the rise since 2005. Then, the threshold was lowered to KRW 10 million from KRW 20 million in June 2010. Currently, there is ongoing legislation concerning the abolishment of the reporting threshold.

c. STR Method and Procedures

Employees at branch offices are required to report suspicious transactions to the reporting officer in the organization if they detect that there are suspicious transactions considering the usual transaction profile of the customer, occupation, the content of businesses based on their expertise, knowledge, and experience.

The reporting officer reviews the information from bank tellers and its own data, and if there are reasonable grounds to suspect that transactions are related to money laundering, he/she reports them to KoFIU without delay.

The reporting officer is required to prepare the name of the reporting entity (financial institutions), customers' information, the reasonable ground for suspicion, the type of retaining information on the standard STR form, which is annexed to the *Financial Transaction Reports Act* (FTRA). The STR form can be filed on-line, in hard copy, or in floppy disks. In urgent cases, it can be filed through FAX or by telephone and supplemented with documentation afterwards.

d. Dissemination of STR to Law Enforcement Agency

KoFIU conducts comprehensive analysis of relevant information based on objective data from related authorities such as foreign exchange networks and credit information, which are not available for financial institutions. If there are any reasonable grounds to suspect that the reported transaction involves money laundering, KoFIU provides a suspicious transaction report (STR) to appropriate law enforcement agencies. The systematic steps facilitate the promotion of financial institutions' participation in STR and the guarantee of secrecy in bona fide financial transactions. For effective operations, it is important to build a channel to share information between the reporting officer and KoFIU, or between KoFIU and law enforcement agencies on a regular basis.

3.2.2. Currency Transaction Report (CTR)

A Currency Transaction Report (CTR) is designed to enhance the effectiveness of preventive measures for the fight against crime by conducting comprehensive analysis based on objective information. In this regard, the CTR complements STR, which determines whether there are suspicious transactions depending on the judgment of financial institutions. Under the CTR, financial institutions are required to report all currency transactions above a designated threshold that is applied to all related entities.

a. The Reporting Threshold and CTR Subject

If transactions total more than KRW 50 million in currency, cash payment or receipt on behalf of the same person from the same financial institution during one business day, they are subject to a Currency Transaction Report (CTR).

A currency transaction is any transaction involving the physical transfer of currency from customers to financial institutions or vice versa. CTR subject includes deposits and withdrawals, automated teller machine (ATM) transactions, and cash transactions deposits through night deposit boxes. However, a CTR is not applicable to transactions when there is only a transport of value such as fund transfers and electronic banking.

The CTR requires all financial institutions to report suspicious currency transactions in relation to money laundering, thereby enhancing the effectiveness of preventive measures for crimes. However, because it could undermine production and transaction activities of businesses that tend to conduct currency transactions, the necessary step is to operate the CTR in a reasonable way.

In response to the concern, Enforcement Decree on the FTRA stipulated that a designated threshold should be KRW 50 million, a higher figure than that of foreign countries, at the early adoption stage of the CTR and it should be lowered on a gradual basis considering economic implications. It recommended that the threshold was lowered at KRW 30 million starting from 2008 and to KRW 20 million staring from 2010. In addition, in regard to the aggregation of currency transactions, there were exemptions for currency transactions totaling less than KRW 1 million wire transfers (deposits without passbooks) conducted on a daily basis, denomination exchanges, and utility bill payments.

Depending on the establishment of the system, regular currency transactions with a low risk of money laundering are likely needed to consider the exemption from reportable transactions in the long term.

b. CTR Filing Requirements

Financial institutions are required to provide all requested information on the CTR, including information on the person conducting transactions such as name and address, and transactions such as transaction date and transaction amount. If financial institutions are likely to file lots of CTRs, they are required to use private networks of intermediary agencies such as the KFB and Securities Dealers Association. Financial institutions with a few CTRs can report over the Internet. In response to security concern, encryption technology including digital certificates are installed into an all reporting system ranging from financial institutions to KoFIU.

3.2.3. Customer Due Diligence (CDD)

A Customer Due Diligence (CDD) requires financial institutions to verify a customer's identity, address, contract number if the customer opens a account or there is an one-off transaction exceeding a designated threshold. Additionally, financial institutions are required to verify a customer's identity and the purpose of transactions if the customer is suspected to be engaged in money laundering; for example, if the beneficial owner is suspicious.

What both the CDD and the real-name financial transaction have in common is that they are designed to improve transparency in financial transactions; however, there is a difference in terms of specific purposes, the applicable scope, and the effect and conditions as follows <Table 1-7>.

Table 1-7 | Real-Name Financial Transaction and Customer Due Diligence (CDD)

Division	Real-Name Financial Transaction	Act on Report on, And the Use of Specific Financial Transaction Information
Purpose	Realization of economic justice and normalization of financial transactions	• Customer Identification
Applicable Scope	• Banking/deposit-taking business • Exchange business, Securities business • Excluding insurance • mutual aid • credit card business	• Real-name financial transaction and Futures Trading Act applied transactions • Financial traders excluding the application of real name including bank credit, insurance, mutual aid, credit card business

Division	Real-Name Financial Transaction	Act on Report on, And the Use of Specific Financial Transaction Information
Subject	• Opening accounts • Wire transfer exceeding KRW 1 million	• Opening accounts • One-off transaction exceeding KRW 20 million • Beneficiary owner is suspicious • Transaction is suspicious of money laundering
Checklist	Individuals with ownership over the account	• Customer's identity (Real name, address, contract number) • Individuals with ownership over the account, purpose of transaction
Verification	It is required to verify a certificate of real-name identification	Financial institutions have the discretion to verify
Measures when Failing to Verify	Financial institutions cannot conduct transactions and they may face fines if there is a violation	• Financial institutions have the discretion to determine whether they continue to conduct transactions or refuse or discontinue • It is possible to file STR after transactions

Source: Korea Financial Intelligence Unit

a. CDD Subject

Financial institutions are required to verify the identity of each customer if the customer opens an account or if there is a one-off transaction exceeding KRW 20 million ($ 10,000), and the detailed contents are as follows:

① Opening New Account

Account opening is when a customer opens an account or consignment sales and purchases account entering into a contract with a financial institution to initiate a financial transaction. It includes, for example, insurance· mutual benefit contract, loan guarantee insurance contract·factoring contraction, certificate of deposit, issuance of cover note, safe deposit box agreement, and fiduciary deposit.

② One-off Transaction exceeding KRW 20 million ($ 10,000)

One-off transaction is a financial transaction carried out without opening an account at a financial institution. It includes, for example, deposits without passbook·wire transfers, foreign currency wire transfers, issuance of a cashier's check, payment of promissory note·checks, and trading of prepaid cards.

b. CDD Requirements

Under Article 10-4 of the *Enforcement Decree of the Financial Transaction Reports Act* (FTRA), financial institutions are required to verify a customer's identity. The customer identity information that financial institutions are required to check for each category of customers is as follows in <Table 1-8>.

Table 1-8 | Customer Identity Information

Division	Customer Identity Information
Individuals	• Real name, address, contract information
For-profit Legal Entities	• Real name, business type, locations of headquarters and offices, contact information, real name of the representative
Non-profit Legal Entities and Other Organization	• Real name, purpose of business establishment, locations of headquarters and offices, contact information, real name of the representative
Foreigners and Foreign Organizations	• Information specified in the corresponding category of the three categories above, nationality, location of local residence or office

Source: Korea Financial Intelligence Unit

Financial institutions are required to verify "individuals with ownership over the account and the purpose of transactions" as well as a customer's identity if the customer is likely to engage in money laundering, including when individuals with ownership over the account is suspicious. Based on knowledge, expertise, and experience, financial institutions make a comprehensive judgment to determine whether the customer is likely to engage in money laundering. Meanwhile, the *Financial Transaction Reports Act* (FTRA) stipulated that individuals with ownership over the account are suspicious are cited as the typical example of the case in which the customer is likely to engage in money laundering.

Financial institutions are required to verify the identity of a customer and then the account's beneficial ownership other than the customer, namely whether the customer has ownership over funds for financial transactions. Accordingly, financial institutions have the discretion to decide the identify of the account's beneficial ownership based on their risk assessment.

Financial institutions should verify the purpose of financial transactions regardless of knowing the true identity of the customer. They should verify the main purpose if there are transactions for various purposes.

c. CDD Procedures

Financial institutions are, in principle, required to verify the identity of each customer before financial transactions occur. In inevitable circumstances arising from the nature of financial transactions, however, they may verify customers' identity after financial transactions and types of transactions are set forth in a supervisory regulation. The verification of customers' identity after financial transactions is allowed under the supervisory regulation: in cases of opening an account for employers or students on a comprehensive basis, if a customer conducts its first financial transaction after opening a new account; in cases of third party insurance under Article 639 of the *Commercial Act*, if a policyholder is claimed for settlement, maturity refund and other settlement, or if a claim for settlement, maturity refund and other settlement is carried out.

Financial institutions are not required to verify a customer's identity when financial transactions are carried out by the same person who is already verified through the identifying procedure. However, the CDD required financial institutions to implement the rule if the existing identifying information is inconsistent with the fact or if the validity is suspicious.

3.2.4. Establishment and Operation of Financial Institution's Internal Control System

In order to promote Suspicious Transaction Report (STR) and effectively prevent money laundering, financial institutions need to establish an internal control system as follows:

① Appointing a reporting officer for STR and establishing an internal reporting system;

② Preparing and operating AML guidelines;

③ Training staff for anti-money laundering; and

④ Reviewing and improving an internal control system and operations.

The structure of the internal control system and the method of operation can vary from financial institutions to regional institutions. Accordingly, the operation is conducted by the preparation of the common operation guideline by financial institutions, joint training, and the exchange of related information. Excluded from the establishment of an internal control system are banks that have no financial transactions for the public or small scale businesses in order to reduce the burden of the establishment.

An appointed compliance officer is required to conduct a comprehensive review in relation to money laundering upon receiving the report on irregular transactions from each branch, and to act as an intermediary to report suspicious transactions to KoFIU. Financial institutions are required to provide employees with training on the types of suspicious transactions, on how to detect and determine whether transactions are suspicious in banks in order to report them. Training materials such as the types of suspicious transactions and reporting guidelines need to be prepared in consultation with financial institutions' representatives, including KoFIU and the Korea Federation of Bankers (KFB).

Money laundering becomes more and more sophisticated and complex methods are being used through a variety of financial instruments. Accordingly, in order to detect suspicious transactions, there is a growing need for adjustments by making regular publications on reporting guidelines and examples for reference.

It goes without saying that the success of an AML regime depends on active participation in the reporting by financial institutions' employees. However, employees in financial institutions may feel a sense of vague anxiety regarding the disadvantages they face when they report suspicious transactions. If customers know that their transactions are reported, they may discontinue to do business with the bank or complain about the report. In addition, reporting puts the burden on employees when they are summoned by KoFIU or investigative agencies summon them for explanations or they are subject to taking accountability. Therefore, institutional measures are taken for the guarantee of secrecy of the report and exemption of reporting to ensure that employees are motivated to carry out their duties without facing any negative repercussions.

Suspicious transaction report does not contain the name of an employee at a bank's branch. The reported content in the analysis process is verified through the reporting officer at the bank's headquarters or assigned personnel. In other words, the reporting operation exterminates when the employee at the bank's branch reports a suspicion to its headquarters.

In addition, exemption of a bank from liability for damages regarding reports, prohibition of accepting specific financial transactions information as evidence in the judicial process, and the right to refuse to testify by the bank's staff are stated under the laws and regulations. Information provided with law enforcement agencies from KoFIU is required to be used as evidence for the investigation along with a combination of several materials. The real-name system for personnel responsible for review and analysis is adopted. Public officials in KoFIU and staff at law enforcement agencies face strict punishment such as imprisonment for not more than five years or a fine of not more than KRW 30 million if they disclose the secrecy of specific financial transactions information or violate the prohibition of use of information for other purposes.

3.3. Progress of Anti-Money Laundering System

Korea was implementing the revision of the *Financial Transaction Reports Act* (FTRA) in June 2012 in order to meet the international standards of the AML system. The following is the main components of the Act, which are intended to remedy deficiencies in the legislation.

3.3.1. Abolishment of Suspicious Transaction Report (STR) Threshold

A designated threshold for Suspicious Transaction Report (STR) under the Article 4 was abolished. In Korea, the designated threshold was KRW 50 million in 2001 when the legislation was enacted and then it was lowered to KRW 20 million in January 2004 through the revision. Currently, the applicable requirement is based on the revision in June 2010. Financial institutions are required to report if there are transactions greater than KRW 10 million or $50 million; however, banks have the discretion to report under the reporting requirement.

However, the FATF international standard requires financial institutions to report transactions to an FIU if there is a suspicion that financial transactions are related to illicit profits·money laundering. Under the circumstance, the FATF recommended that Korea abolish the threshold. Korea has recently accepted the recommendation. Thus, financial institutions are required to abolish the threshold and report regardless of transactions amount if transactions are suspicious.

There is some concern about an increasing number of STR cases if the reporting requirement is abolished. However, the threshold does not play a role because financial institutions report transactions below KRW 10 million regardless of the threshold after sampling and reviewing through a monitoring system. Transactions below KRW 10 million represent about 5% to 6%. The mere abolishment of the threshold could have little impact on financial transactions irrelevant to illicit profits · money laundering activity as shown in <Table 1-9>.

Table 1-9 | STR Status

	2007	2008	2009	2010	2011	2012 1 ~ 4
Monthly Average Report (case) (A)	4,373	7,674	11,357	19,672	27,455	23,289
Below KRW 10 million (case) (B)	606	963	1,065	1,099	1,389	1,302
Share (%) (B/A)	13.9%	12.6%	9.4%	5.6%	5.1%	5.6%

※ The full adoption of the monitoring system from 2008 to 2009 led to the development of STR sampling function, thereby relatively reducing transactions below KRW 10 million

Source: KoFIU

3.3.2. Grounds for Providing Sender's Information When Using Wire Transfer

There is no regulation concerning the provision of the sender's information when using wire transfers under the laws and regulations. However, the sender's information is provided with the consent of the sender when using international wire transfer; name or account number of the sender are provided when using local wire transfer.

However, the FATF required the sender's bank to provide name, account number, address or resident registration number to the recipient's bank in order to combat AML/CFT using wire transfer. The purpose of legislating the Article 5-3 is to respond to this conditions.

This enables Korea to enhance an AML framework complying with the international standard and take effective countermeasures for money laundering activity using separate wire transfers.

Besides, for enhanced personal information security, types of reference data for review and analysis were added in the regulation, such as the family registration card stated in Enforcement Decree. The above revisions were already completed prior to the announcement of legislation from June 13, 2012 to July 23, 2012 and they have been submitted to the National Assembly for review by the Regulatory Reform Committee, the Ministry of Government Legislation.

Chapter 2

Implementation Strategies of the FIU Information System

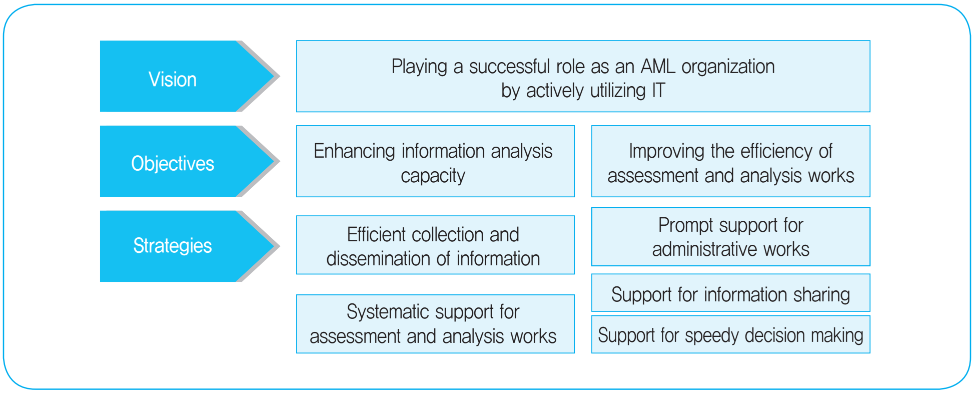
Implementation Strategies of the FIU Information System

1. Implementation Summary of the FIU Information System

The Korea Financial Intelligence Unit (KoFIU) set up a policy of actively utilizing information technology (IT) to establish a systematic and efficient anti-money laundering (AML) framework when it was launched on November 2001, and adopted an informatization vision “playing a successful role as an anti-money laundering organization by actively utilizing IT” shown in [Figure 2-1] below.

In order to meet this goal, KoFIU has established two objectives: (i) enhancing information analysis capacity; and (ii) improving the efficiency of assessment and analysis works. Also, in order to effectively accomplish these objectives, it has adopted five strategies: (i) efficient collection and dissemination of information; (ii) prompt support for administrative works; (iii) systematic support for assessment and analysis works; (iv) support for information sharing; and (v) support for speedy decision making.

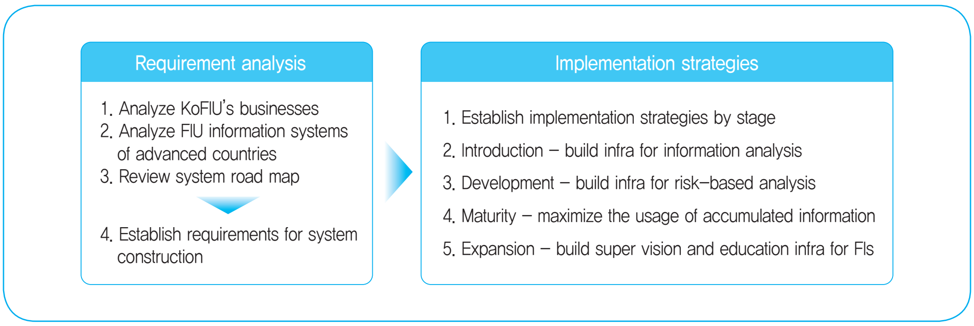
Figure 2-1 | KoFIU's Informatization Vision



Source: Korea Financial Intelligence Unit

To carry out the informatization project in line with the above five strategies, KoFIU analyzed requirements for construction of the FIU Information System, and established its implementation strategies accordingly. The summary of implementation is described in [Figure 2-2] below.

Figure 2-2 | Implementation Summary of the FIU Information System



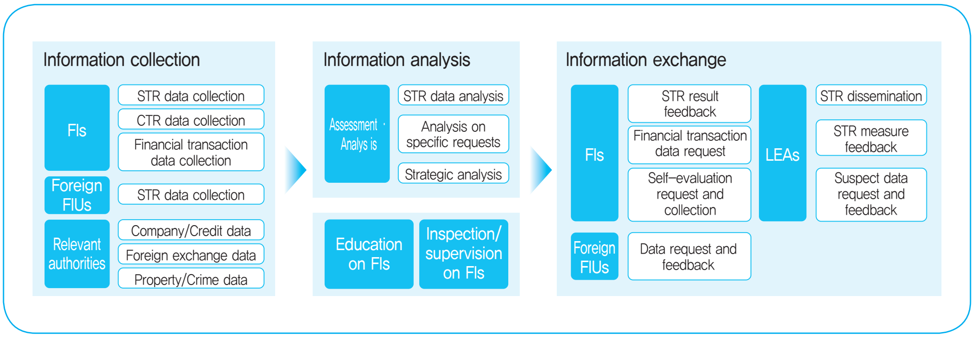
To analyze the requirements for constructing the FIU Information System, KoFIU conducted the following work. First, KoFIU analyzed its business as an AML agency, and identified the necessary functions to perform the business. Second, it reviewed FIU systems of advanced countries, and analyzed their systems' requirements and construction paradigms. Third, in order to become a regular member of the FATF, KoFIU sped up the adoption period of the system in consideration of the FAFT Recommendations, and reviewed the system construction period. Finally, it drew up requirements for system construction by analyzing KoFIU's business and FIU systems of advanced nations, reviewing the road map of an

AML framework, etc. Also, based on the requirements, it set up implementation strategies by stages, ting into account significance aspects (construction urgency and efficiency, etc.) and feasibility aspects (costs, technological sophistications, etc.).

1.1. Analysis of KoFIU's Business

KoFIU works as an institutional link between financial institutions (FIs) and law enforcement agencies (LEAs) with regard to transaction information related to money laundering (ML) or funds for offences of public intimidation. KoFIU analyzes STRs from FIs and disseminates the most suspicious transaction information to LEAs, thereby preventing the direct collision between them and playing a pivotal role in implementing the AML system. Also, it is committed to promoting international cooperation and adopting new systems in line with global trends. KoFIU's work processes are shown in [Figure 2-3].

Figure 2-3 | KoFIU's Work Flowchart



Source: Korea Financial Intelligence Unit

① Information Collection

KoFIU receives transaction information regarding criminal funds from FIs as well as data necessary to analyze the information from relevant authorities, in turn building a comprehensive database for the suspect. The comprehensive database consists of STR/CTR from local FIs, financial transaction information from foreign FIUs, foreign exchange information, relevant authorities' information for analyzing the data, information from credit information companies, etc.

In order to upgrade the quality of information analysis, information collection is crucial. When establishing a data warehouse, the information collected from FIs should be reprocessed and applied to the works of KoFIU, and data received from relevant agencies should be upgraded on a regular basis to maintain their reliability.

In addition, since the accuracy of STR is of utmost importance, KoFIU should conduct consistent monitoring and training for reporting personnel of FIs as well as regular audits on STRs.

② Information Analysis

For financial transactions suspected to be related to crimes as a result of comprehensive data analysis, KoFIU provides analysis results to LEAs. Information analysis comprises operational analysis, tactical analysis and strategic analysis as shown in <Table 2-1>.

Table 2-1 | Types of Information Analysis

Type	Analysis content
Operational Analysis	To analyze suspicious levels of STRs reported by FIs
Tactical Analysis	To analyze specific individual, group or matter for the purpose of indictment, etc.
Strategic Analysis	To analyze a big picture such as overall trends, patterns, geographical characteristics and forms, etc. rather than specific matters

Source: Korea Financial Intelligence Unit

To effectively carry out various types of information analysis, analytical tools are necessary to draw a big picture of the whole financial transaction trends by linking STRs to collected data. For example, the U.S. is employing advanced analytical tools such as link analysis and OLAP, using IRS information, crime data, etc., to determine whether STRs are reliable.

③ Information Exchange

KoFIU receives and arranges feedback from LEAs for information it provides, and offers statistics and analyzes outcomes of STRs to FIs. Consistent feedback is essential to identifying and preventing ML crimes. In particular, accumulated feedback from investigative agencies can improve the efficiency of information analysis.

1.2. Analysis of FIU Systems of Advanced Countries

The FIU system of the U.S., currently operated by FinCEN, consists of an information analysis mart (based on information collected from various internal and external sources) and an artificial intelligence-based analysis system (developed to figure out ML techniques). This system is focused on comprehensively analyzing the whole information by linking currency transaction, suspicious transaction and foreign exchange transaction information to the suspect, transaction and account data, rather than analyzing suspicious transactions case by case.

① Information Collection

FinCEN collects SARs from FIs through an E-filing system. In terms of CTR, FIs report them to the IRS, and then FinCEN collects the information on-line from the IRS. Also, commercial and law enforcement data such as each state's public data and credit/identification/finance/crime data are collected on-line through pre-determined data formats.

② Information Analysis

Information analysis is largely divided into a data driven operation and a user directed analysis.

The data driven operation is to automatically assess all new information inputted into the databank through an artificial intelligence-based analysis system. The operation is implemented in the following order: data transfer from the U.S. Customers Service datacenter → information consolidation by program → information classification by transaction, account and person → information linking based on common information derived from person, company or account data → assessing suspicious levels with 336 analysis rules → totaling suspiciousness scores.

The user directed analysis is for evaluators to directly employ analytical tools, using the wagon wheel display (a method to display financial transaction relations of each entity (transaction, account and person)) or the link & edge display (a method to display the just-above relations plus geopolitical location).

③ Information Exchange

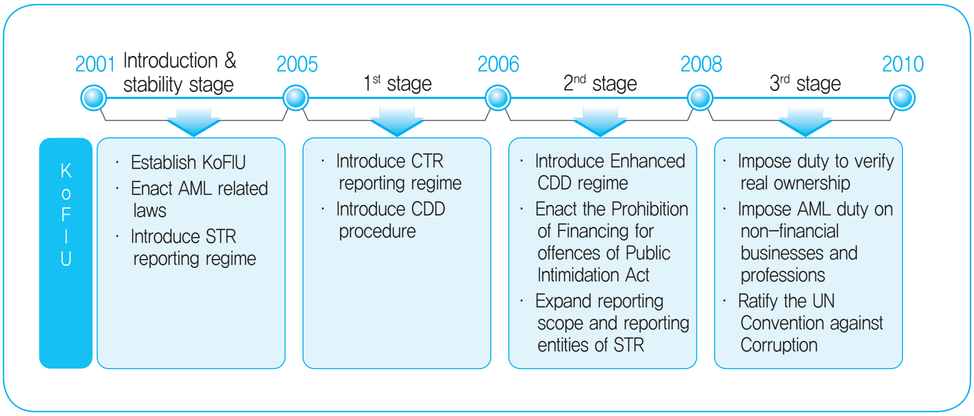
Information sharing is divided into three ways: (i) direct support method to directly provide information requested by LEAs; (ii) platform support method in which LEAs dispatch their part-time workers to FinCEN and let them collect and utilize necessary information; and (iii) on-line support system to have LEAs directly search and use necessary information on FinCEN's website.

In particular, the Gateway System utilized in the on-line supporting system allows LEAs to access FinCEN's financial databank, enabling investigative agencies to use a wide range of information. This information sharing system was first run in Texas on a trial basis, and is expanding into other states after its utilization rate was found to exceed more than 60% of the whole investigations conducted in the state. Also, the Gateway System stores all questions, compares previous surveys with current questions, and when an inputted suspect is identified in previous questions, informs that to the current user, thus avoiding repetitious investigative works and making it possible for inspectors to share investigation processes for an identical suspect.

1.3. Review of System Road Map

In order to meet strengthened AML-related international standards and actively respond to domestic demand for system improvement, KoFIU had a series of working-level meetings and discussions with the Ministry of Justice (MOJ), Financial Supervisory Commission (FSC), etc. and has adopted the "road map for implementation of the FATF Recommendations" with the aim of achieving phased system improvements shown in [Figure 2-4].

Figure 2-4 | Road Map for Implementation of FATF Recommendations



Source: Korea Financial Intelligence Unit

The first stage was scheduled to complete in 2005, covering the follow-up actions of the introduction of CDD and CTR systems. In short, the stage aimed to reflect concrete implementation procedures and reporting forms in lower-level regulations, as well as to adopt related electronic systems.

The second stage, scheduled from 2006 to 2007, dealt with enacting legislation on combating terrorist financing, expanding STR obligation to terrorist funds, fostering education and training for personnel in charge of AML activities, etc.

The third stage, set from 2008 until 2010, covered levying AML obligations on non-financial businesses and professions, expanding the scope of predicate offences for ML, enacting legislation necessary to ratify the UN Convention Against Corruption, etc.

1.4. Establishment Requirements of the FIU Information System

The FIU Information System led by KoFIU provides the following functions to reinforce the information analysis capacity and improve the efficiency of assessment and analysis work: (i) efficient information collection and dissemination during data collecting, analyzing and sharing processes; (ii) prompt support for administrative works; (iii) systematic support for assessment and analysis works; and (iv) support for speedy decision making.

The basic principle of construction of the system is to build a system that can efficiently help the soft-landing of the AML regime in line with the "road map for implementation of FATF Recommendations." For this, KoFIU classified the functions necessary to build the system into 14 categories, and set out a total of 48 detailed requirements for each category as shown in <Table 2-2>.

Table 2-2 | Construction Requirements of the FIU Information System

Category	Requirements
Report Collection	Formulate STR, CTR forms
	Build STR, CTR on-line systems
	Build a security system for on-line STR, CTR systems
Access to Information	Collect financial transaction information
	Collect related administrative information
	Collect law enforcement information
Assessment/ Analysis	Measure STR suspicious levels and prioritize STRs
	Control data necessary for STR process
	Build database for information control and analysis
	Collect STR, CTR data from FIs
	Collect data from foreign FIUs
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
Information Exchange	Collaborate with relevant local authorities and conduct knowledge management
	Disseminate analysis reports to LEAs
	Formulate forms for additional data request
	Automate information exchange process
	Provide ML/TF trends and scenarios to FIs
	Offer feedback on law enforcement reports

Category	Requirements
Information Exchange with Foreign FIUs	Formulate data exchange forms with foreign FIUs
	Automate data exchange process with foreign FIUs
	Automatic data reconciliation with foreign FIUs
Registering Reporting Personnel	Control the list of FIs
	Control the list of reporting personnel
Raising Awareness of Reporting Entities	Build contact channels (portal site, etc) with reporting entities (FIs)
	Share exemplary cases of reporting entities
	Provide feedback to reporting entities
	Build an education control system
Information Security Control	Conduct security risk assessment
	Establish data security policies and organization
	Control information assets
	Secure physical and environmental securities
	Enhance access control
	Build, develop and maintain information system
	Control accidents related to information security
	Provide anti-virus software
Strategic Analysis	Provide strategic analysis scenarios
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
Inspection/ Supervision	Prepare inspection guidelines and checklists
	Conduct risk assessment on FIs
	Inspect compliance with regulations
Information Processing	Conduct data validity test
	Conduct rules-based validity test
	Conduct validity test on external sources
	Inform reporting entities (FIs) of data validity test results
Performance Control	Build performance control process and carry out performance control
Information Control	Control information architecture
	Control documents
IT Infra Control	Control IT infra

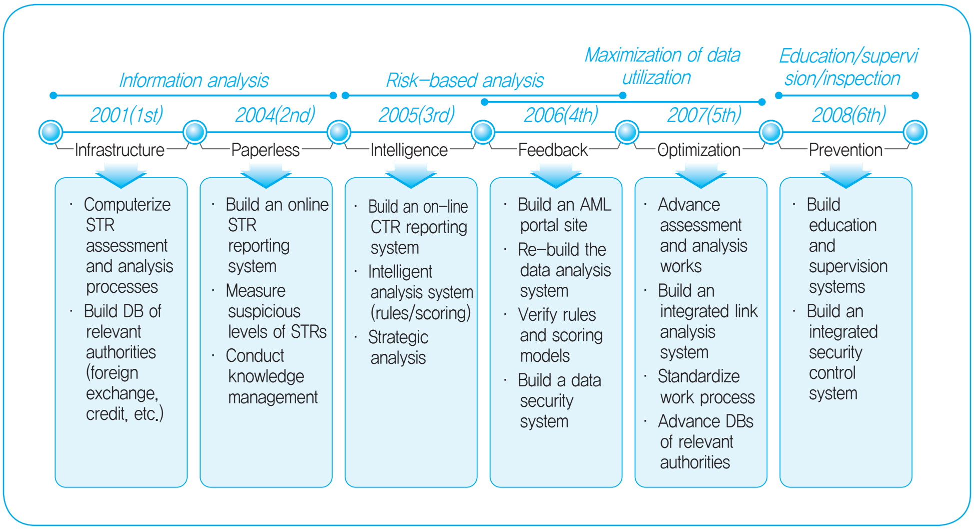
Source: Korea Financial Intelligence Unit

2. Implementation Strategies of the FIU Information System

2.1. Establishment of Implementation Strategies by Stage

Based on construction requirements for the FIU Information System, KoFIU set up mid- and long-term implementation strategies from 2002 to 2008, considering significance aspects (construction urgency, efficiency, etc.) and feasibility aspects (costs, technological sophistication, etc.). The strategies are set out in [Figure 2-5] below.

Figure 2-5 | Implementation Strategies by Stage



Source: Korea Financial Intelligence Unit

The mid- and long-term implementation strategies classified the construction process into four stages: introduction (establishment of information analysis infra) → development (establishment of risk-based analysis infra) → maturity (maximization of utilization of accumulated information) → expansion (establishment of supervision and education infra over FIs). Implementation period for each stage was one to two years. Also, considering evolving financial transaction techniques, changing financial environments and change in KoFIU's work efficiency and workload, detailed implementation tasks were set out for each stage.

2.2. Introduction Stage: Establishment of Information Analysis Infrastructure

The introduction stage aimed to establish infrastructure for information control and analysis, and were carried out through the first and second projects. Primary construction requirements of this stage are shown in <Table 2-3>.

The first project put an emphasis on building basic infrastructure, including work processes so that KoFIU, launched in 2001, can play its role as a primary AML organization. The 2nd project focused on building a speedy decision-making support system such as the internal electronic approval system, as well as fixing the inefficient data collection process resulting from increased STRs in 2004.

Table 2-3 | Construction Requirements of the Introduction Stage

Category	Requirements
Report Collection	Formulate STR form
	Build a STR on-line system
	Build a STR on-line security system
Access to Information	Collect financial transaction information
	Collect related administrative information
	Collect law enforcement information
Assessment/Analysis	Control data necessary to deal with STRs
	Build database for information control and analysis
	Collect STRs from FIs
	Collect data from foreign FIUs
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
Information Exchange	Collaborate with relevant local authorities and conduct knowledge management
	Disseminate analysis reports to LEAs
	Provide ML/FT trends and scenarios to FIs
Information Exchange with Foreign FIUs	Formulate data exchange forms with foreign FIUs
	Automate data exchange process with foreign FIUs
	Automatic data reconciliation with foreign FIUs
Registering Reporting Personnel	Control the list of FIs
	Control the list of reporting personnel

Category	Requirements
Raising Awareness of Reporting Entities	Share exemplary cases of reporting entities
Information Security Control	Enhance access control
	Build, develop and maintain information system
	Provide anti-virus software
Information Control	Control documents
IT Infra Control	Control IT infra

Source: Korea Financial Intelligence Unit

2.3. Development Stage: Establishment of Risk-based Analysis Infrastructure

The development stage aimed to change the existing FIU Information System from man-based to system-based by carrying out efficient analysis of CTR data, building an intelligent analysis system, re-designing information control and analysis processes, etc. Primary construction requirements of this stage are shown in <Table 2-4> below.

Table 2-4 | Construction Requirements of the Development Stage

Category	Requirements
Report Collection	Formulate CTR form
	Build a CTR on-line system
	Build a CTR on-line security system
Assessment/Analysis	Measure STR suspicious levels and prioritize STRs
	Build database for information control and analysis
	Collect CTR data from FIs
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
Strategic Analysis	Provide strategic analysis scenarios
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)

Source: Korea Financial Intelligence Unit

2.4. Maturity Stage: Maximization of Utilization of Accumulated Information

The maturity stage aimed to improve analysis efficiency by building efficient communications networks among relevant agencies, advancing analysis work and improving work processes. To this end, the stage was carried out through the fourth and fifth projects as shown in [Figure 2-5]. The construction requirements of this stage are in <Table 2-5>.

The fourth project was focused on advancing assessment and analysis systems, building an information security system and establishing networks among related agencies for effective communications. As newly-adopted systems such as Enhanced CDD led to an explosive increase in the number of STRs, the fifth project placed an emphasis on greatly improving the flows of information and work process by upgrading the FIU Information System to be more adaptable to the rapidly changing environments.

Table 2-5 | Construction Requirements of the Maturity Stage

Category	Requirements
Assessment/Analysis	Measure STR suspicious levels and prioritize STRs
	Build database for information control and analysis
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
	Disseminate analysis reports to LEAs
	Formulate forms for additional data request
	Automate information exchange process
	Offer feedback on law enforcement measure reports
Registering Reporting Personnel	Control the list of FIs
	Control the list of reporting personnel
Raising Awareness of Reporting Entities	Build contact channels (portal site, etc) with reporting entities
	Provide feedback to reporting entities
	Build an education control system
Information Security Control	Conduct security risk assessment
	Establish data security policies and organization
	Control information assets
	Secure physical and environmental securities
	Control accidents related to information security

Category	Requirements
Strategic Analysis	Provide strategic analysis scenarios
	Conduct artificial intelligence analysis (multi-dimensional analysis, link analysis, etc.)
Information Processing	Conduct data validity test
	Conduct rules-based validity test
	Conduct validity test on external sources
	Inform reporting entities of data validity test results

Source: Korea Financial Intelligence Unit

2.5. Expansion Stage: Establishment of Supervision and Education Infrastructure over FIs

The expansion stage aimed to build infrastructure for guidance and supervision for AML activities of FIs, as well as to enhance the security of data retained by KoFIU. <Table 2-6> shows construction requirements of this stage.

Table 2-6 | Construction Requirements of the Expansion Stage

Category	Requirements
Information Security Control	Conduct security risk assessment
	Secure physical and environmental securities
	Enhance access control
	Control accidents related to information security
Inspection/Supervision	Compose inspection guidelines and checklists
	Conduct risk assessment on FIs
	Inspect compliance with regulations

Source: Korea Financial Intelligence Unit

Chapter 3

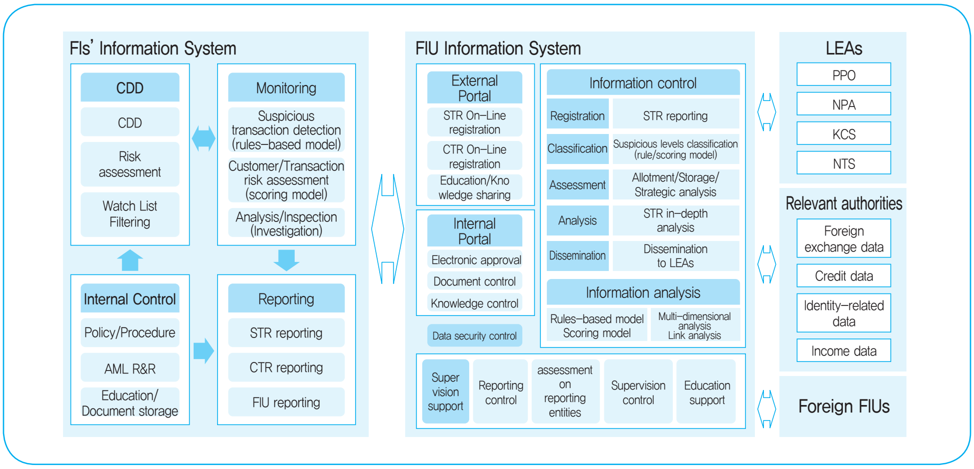
Implementation Progress of the FIU Information System

Implementation Progress of the FIU Information System

1. Current Establishment Status of Information Systems of KoFIU and FIs

The anti-money laundering system is a comprehensive ML risk control system, connecting KoFIU, FIs, LEAs and foreign FIUs. In short, in order to effectively prevent ML activities, it is necessary to build information networks between KoFIU and relevant organizations. The roles and current states of each entity in the AML information network, built in accordance with implementation strategies described in Chapter 2, are set out in the following [Figure 3-1].

Figure 3-1 | Current Status of the AML Information Network



Source: Korea Financial Intelligence Unit

First of all, financial institutions construct and operate their own information systems in which they manage customers through their risk-based monitoring systems, spot suspicious transactions through transaction monitoring systems (consisting of rules-based technology or scoring technology), and report them to KoFIU.

KoFIU also constructs and operates its own 'FIU Information System' which collects STRs from about 6,000 FIs through an online STR reporting system, classifies and assesses their suspiciousness levels, conducts in-depth analysis and disseminates data to LEAs. In particular, the FIU system automatically collects external administrative information such as credit and identity-related data necessary for in-depth analysis from relevant authorities.

And law enforcement agencies are provided with suspicious transaction data from KoFIU via their electronic document systems, and conduct additional investigations on the data and file an indictment if there are any suspicions.

Lastly, for information exchange with foreign FIUs, KoFIU offers and requests suspicious transaction data via the Egmont Secure Web (ESW), which was developed for information exchange among FIU entities and is operated by FinCEN of the U.S.

Review on establishment status of the AML information network has proven that the networks among KoFIU, FIs, relevant authorities and foreign FIUs are being effectively operated via encoded on-line network systems, but the on-line data exchange system with LEAs is not entirely satisfactory.

This chapter explores the current establishment status of the information systems of KoFIU and FIs, the two pillars of the information network, together with detailed implementation processes of each project.

1.1. Establishment Status of KoFIU's FIU Information System

KoFIU has carried out eight projects for construction and improvement of the FIU Information System in accordance with implementation strategies it adopted. The first to sixth projects were mainly conducted to build basic infra of the AML system as well as to improve system efficiency. And the seventh and eighth projects emphasized enhancing security and improving the system. The FIU Information System took its shape through the first to sixth projects. The purpose of establishment, implementation details, achievements and improvements of each project is provided in section 2 of this chapter. The section will review the main systems of KoFIU's FIU Information System.

To effectively implement AML activities, KoFIU built the Korea Financial Intelligence System (KoFIS), which was launched on November 28, 2002, by combining the merits of advanced countries' AML systems (information control and analysis, etc.) with the characteristics of local financial systems (real-name financial transaction system, rapid on-line transactions, etc.). The purpose of KoFIS is to analyze suspicious transaction data more accurately and provide them to LEAs more promptly. As shown in [Figure 3-1], KoFIS is made up of six subsystems: information control system, information analysis system, external portal system, internal portal system, security control system and supervision support system.

1.1.1. Information Control System

The information control system is designed to control the flow of information, or registration → classification → assessment → analysis → dissemination. The key functions of the system are ① to measure suspicious levels using rules-based and scoring models, etc. and intelligently identifying transactions with higher suspicious levels (assessment/analysis function); ② to automatically search, once a STR is filed by FIs, whether other STRs exist involving the suspected person or account (search function); ③ to automatically search administrative data (identity and crime-related data, etc.) and financial data (foreign exchange transaction, etc.) for the suspect and provide them to analysts; and ④ to provide additional information to analysts such as CTR, foreign exchange transactions, the cross-border transportation of currency and bearer negotiable instruments, individual credit data, company data, administrative data, etc.

1.1.2. Information Analysis System

The information analysis system supports data analysis by combining STR data with other information such as foreign exchange and credit data collected by KoFIU. Also, the system includes integrative search, multi-dimensional analysis and link analysis functions in order to support various types of analyses described in <Table 3-1>.

1.1.3. External Portal System

The external portal system serves as a medium for KoFIU and FIs to exchange STR and CTR online in predetermined formats as well as information about the operation of the AML system. The key functions of the system are ① to inspect the validity of data to prevent input errors when information is inputted (data validity inspection function); and ② to control network security as well as authentication for system access to secure confidentiality of reported materials (network security and authentication control function).

1.1.4. Internal Portal System

The internal portal system serves as a gateway for analysts and employees of KoFIU to access each function of the KoFIS. Also, it improves work efficiency by offering electronic approval, document control, and knowledge management functions.

1.1.5. Security Control System

The security control system is designed to protect core equipment (hardware, etc.) and data, and is divided into physical, technical and administrative securities.

1.1.6. Supervision Support System

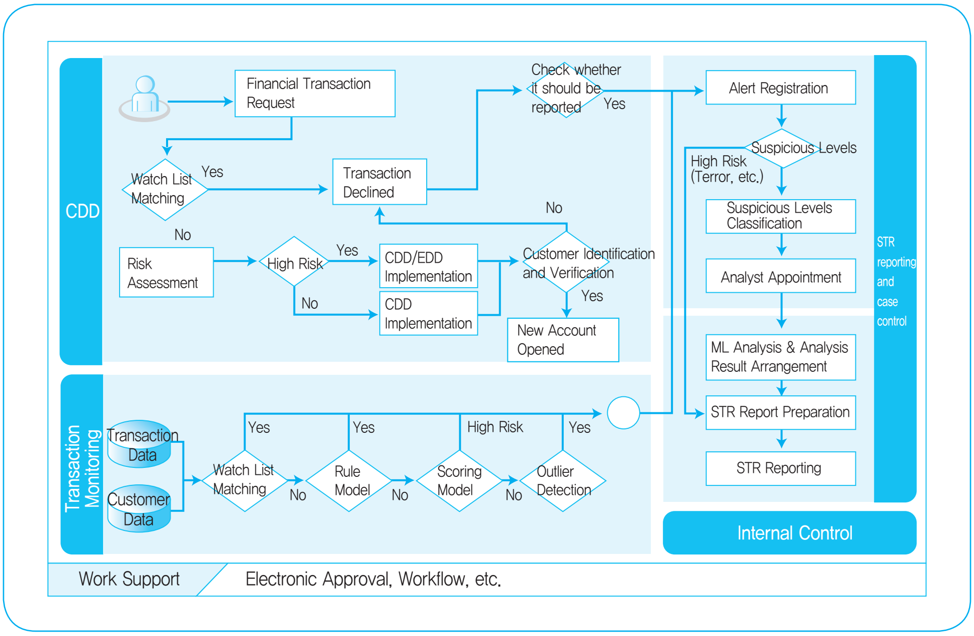
The supervision support system is designed to support education and inspection on FIs. The key functions of the system are (i) to help FIs self-evaluate the appropriateness of operations of their own AML systems (self-evaluation function); (ii) to control supervision schedules and results (supervision control function); (iii) to assess FIs' exposure to ML risk (reporting entities assessment function); and (iv) to control education results on FIs (education support function).

1.2. Establishment Status of FIs' Information Systems

Since the enforcement of the STR regime in 2001, FIs in Korea filed STRs offline (mailings, etc.) until the completion of the Second FIU Information Project in 2004. But with a STR on-line system built in the second project, banks began to actively build their own transaction monitoring systems based on the STR on-line system and rules-based technology, while non-banking financial institutions such as securities and insurance companies lagged far behind banks in placing relevant systems in place.

In 2007, the Korean government pushed forward the revision of laws concerning Enhanced CDD, designation of restricted persons in financial transactions and prohibition of financing for offences of public intimidation as part of Korea's efforts to be a full member of the FATF. In response to this effort, non-banking financial institutions and special banks as well as banks, except only a few FIs, completed the construction of their own AML information systems, starting from 2008 through 2010. The information systems built by each institution vary in detailed compositions and functions depending on each entity's IT environments, but in general consist of a CDD system, transaction monitoring system to spot suspicious dealings, STR and CTR reporting systems, internal control system to monitor the effective operation of the system, and a work support system including electronic approval. The general composition and work flow of the information system are set out in the following [Figure 3-2].

Figure 3-2 | Work/System Flows of FIs' Information System



Source: Samil PricewaterhouseCoopers

The CDD system is designed to effectively control and support the implementation of the Enhanced CDD procedure. The key functions of the system are ① to identify and assess customers' exposure to ML risk using nationality, customer, product and service information (risk assessment function); ② to identify and prevent transactions with individuals or legal entities related to money laundering and terrorist financing (ML/TF) that are on the United Nations Consolidated List, OFAC List, etc. (watch list filtering function); and ③ to automatically control processes in which once a customer is classified into a high-risk group through risk assessment and watch list filtering functions, the program automatically rejects the transaction or conducts the Enhanced CDD procedure (process control function).

The transaction monitoring system plays a role of regularly analyzing customer and transaction data to spot suspicious dealings. To effectively detect suspicious transactions, the system utilizes various analysis techniques such as rules-based technology, outlier detection, scoring technology and watch list filtering shown in the following <Table 3-1>.

Table 3-1 | Analysis Techniques of the Transaction Monitoring System

Technique	Content
Rules-Based Technology	• Detect suspicious transactions based on specific transaction or action rules, such as transactions exceeding a designated threshold or the frequency of divided transactions for a specific period • Constant updating is necessary to reflect changing financial transaction conditions and environments
Outlier Detection	• Classify peer groups according to age, career, etc. and generate profiles for each group. And then, when a transaction occurs, compare the customer subjected to analysis to the profile of his peer group to detect suspicious dealings • Detect known or unknown outlier transactions by identifying transaction patterns
Scoring Technology	• Conduct scoring based on ML risk factors such as transaction, customer, country, etc. and figure out risk levels according to the scoring results
Watch List Filtering	• FIs compare their customer's name to terrorist and criminal watch lists

Source: Samil PricewaterhouseCoopers

The STR and CTR reporting systems aim to control the reporting process of suspicious transactions, or registration → allotment → analysis → reporting. The key functions of the system are ① to notify, once a transaction is suspected to be related to ML/TF through transaction monitoring, this to the manager/inspector/law-abiding monitor (alert management function); and ② to support assessment and analysis for notified transactions, and to automatically report them to KoFIU once they are judged to be suspicious transactions (case management function).

2. Implementation Progress of the FIU Information Project

2.1. The First Project (Infrastructure): Establishment of an STR Analysis System

2.1.1. Purpose of Establishment

The first FIU Information Project aimed to build basic infrastructure for KoFIU's AML/CFT activities, or preventing illegal foreign currency flows and ML activities, playing its role as a primary executive agency to tackle the ML/TF activities. The core requirements to achieve that goal are as follows.

First, in order to implement the STR obligation required by the AML legislation passed in September 2001 such as the *Financial Transaction Reports Act and the Proceeds of Crime Act*, it was necessary to set up information infrastructure, including reporting forms and a data warehouse.

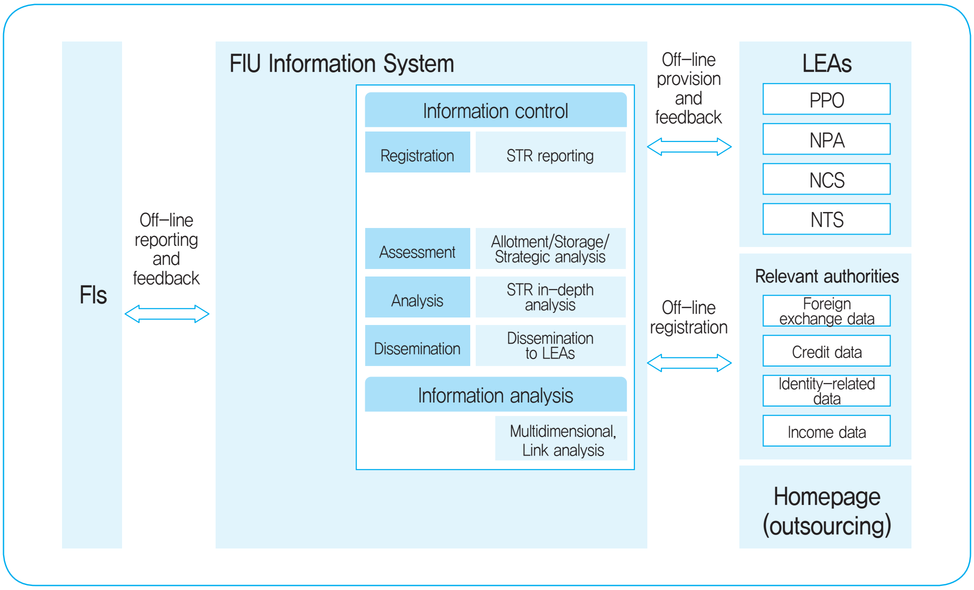
Second, KoFIU needed to automate work processes in order to play a central role in the AML/CFT efforts set out in the AML-related laws. The laws define the roles of KoFIU as analyzing STRs provided by FIs and, when it finds reasonable grounds to suspect that the reported transaction is related to ML, disseminating the STR to an appropriate LEA. Therefore, the first project focused on automating the analysis process, in particular the operational analysis process, among the information collection, analysis and exchange process.

Third, it was also necessary to set up a master plan for the FIU Information System. For the FIU system to be built, large-scale investments were a necessity. And such investments cannot be drawn without a long-term master plan.

2.1.2. Implementation Details

The scope of the first FIU Information Project is to establish a master plan, the FIU Information System, data warehouse, IT infrastructure and a computer center, homepage, etc. The composition of the FIU Information System is set out in the following [Figure 3-3].

Figure 3-3 | Composition of the FIU Information System of the First Project



Source: Korea Financial Intelligence Unit

a. Establishment of Master Plan

The purpose of the master plan is to define implementation directions and work requirements prior to carrying out the FIU Information Project. The master plan set out an implementation vision and strategies, established work process, and drew up work requirements necessary to build an information infrastructure. When establishing the work process, it not only defined the STR dealing process (registration → classification → assessment → analysis) but also drew up requirements for data interface with relevant authorities, for introducing and employing various analysis tools for operational analysis, etc.

b. Establishment of the FIU Information System

The FIU Information System consists of two unit systems: the information control system and the information analysis system.

The information control system controls work processes from registration of STRs to dissemination to LEAs. Also, it manages completed documents in a systematic way.

The information analysis system helps analysts conduct multi-dimensional or link analysis using a variety of information stored in data warehouses such as suspicious and foreign exchange transactions data, credit data, etc. The multi-dimensional analysis is a technique to analyze customers, transactions and accounts in various perspectives, while the link analysis is to figure out relationships of separate entities (customers, accounts, etc.) by showing their relations with symbols such as arrows.

c. Establishment of Data Warehouse

The first project built a comprehensive information analysis database, which helps analysts conduct multi-dimensional and link analysis in various perspectives (customer, account, transaction, etc.) by systematically managing STRs filed on disk as well as information collected from relevant authorities. When the first project was completed, information exchange with relevant authorities was still carried out offline since an online system was yet to be adopted.

d. Establishment of IT Infrastructure and Computer Center Environments

The first project not only designed the structures of hardware, network and data necessary for operation of the FIU system but also established security policy and infrastructure for a system security. In addition, it enhanced access security on IT infrastructure and constructed computer centers for the stable operation of the FIU system.

e. Creation of Homepage

The first project emphasized promoting the newly-adopted AML system, and commissioned an outside facility to create KoFIU's homepage in order to introduce KoFIU to the general public and FIs responsible for the STR obligation.

2.1.3. Achievements of System Establishment

The first project built an infrastructure for information collection and analysis among KoFIU's information collection, analysis and exchange duties. Success factors and major achievements of the first project can be summed up as follows.

a. Minimization of System Vacuum through Advance Preparation

In September 2001, the AML-related legislation such as the *Financial Transaction Reports Act* and the *Proceeds of Crime Act* was passed in the National Assembly. Since then, in order to minimize the system vacuum until the completion of the STR reporting network, the first project organized a Task Force Team (TFT) on the AML activities under the Ministry of Finance and Economy in April 2000, and set up the 'Basic Plan for the FIU Information System' in December 2000. And in June 2001, 'Implementation Strategies of the FIU Information System' was introduced. Thanks to such advance preparations, KoFIU was able to embark on the development of the FIU Information System by November 2001, when it was established without any delays. In addition, so as to effectively implement the STR reporting regime adopted in September 2001, the first project defined the STR form in advance in June 2001 when establishing implementation strategies and distributed it to FIs, thereby minimizing the system vacuum involving the STR regime.

b. Establishment of the Master Plan for Systematic Construction of the FIU Information System

The first project, in accordance with 'Implementation Strategies of the FIU Information System' adopted in June 2001, established short-term and long-term master plans for construction of the FIU Information System by analyzing KoFIU's duties and referring to exemplary cases of advanced countries.

c. Building Infrastructure for Information Networks with FIs

Before an on-line information network with FIs was established, the first project made a standardized STR program and distributed it to reporting entities, and had them submit STRs in hard copy and disk format, in turn reducing input errors resulting from manual work, and efficiently utilizing human resources. The number of STR filings was 275 in 2002, but with the distribution of the program, the number soared to 1,744 in 2003, a 6.3-fold increase.

Table 3-2 | The Number of STR Filings in 2002, 2003 by Month

(Unit: case)

Month	1	2	3	4	5	6	7	8	9	10	11	12	Total
2002	16	11	11	14	15	11	6	15	21	38	64	53	275
2003	74	92	75	105	77	94	184	133	162	247	195	306	1,744

Source: KoFIU

d. Establishment of the Support System for Information Control and Analysis

The first project built an infrastructure for information control and analysis to effectively handle information flow, or STR collection, analysis and dissemination to LEAs. Also, the project not only established a systematic information analysis system but also introduced various analysis techniques such as a multi-dimensional link and link analysis that utilize massive foreign exchange transaction data, credit data, etc.

2.1.4. Improvements

The first project built an infrastructure for the FIU Information System, but with the work process and system being built in a short time, it failed to reflect changes in processes and regimes that occurred during the first project. Needed improvements can be summarized as follows.

a. Low Utilization of the FIU System

The FIU Information System developed in the first project was designed to facilitate assessment and analysis work, so its use was limited to analysts. Also, as assessment and analysis results were printed out and stored in hard copy, the utilization rate of the system was relatively low. This was partly because information exchange with LEAs was conducted in hard copy until the adoption of their electronic document systems.

b. Necessity to Build an On-line Information Network

In the FIU system, STR filing by FIs, dissemination to LEAs and collection of administrative information from relevant authorities was all carried out offline such as mailings. So, in order to improve efficiency of information flows, it was necessary to build an on-line information network.

2.2. The Second Project (Paperless): Establishment of an Online Reporting System

2.2.1. Purpose of Establishment

The purpose of the Second FIU Information Project is (i) to improve the efficiency of information collection to cope with a sharp rise in the number of STR filings in 2004; and (ii) to build a rapid decision-making support system including the internal electronic approval system. The core requirements to achieve the goals can be summed up as follows.

First, it was necessary to improve the STR registration system. The number of STR filings was 275 in 2002. But with the introduction of the AML regime, the number soared to 4,680 in 2004, a 17-fold increase. But STR registration was still carried out in hard copy printed out from the standardized STR program distributed to FIs, thus undermining the efficiency of information flow such as information collection and analysis. Also, the paper form registration brought about security issues such as missing or leaking of STRs.

Second, KoFIU needed to increase the number of analysts. Despite an explosive increase in the number of STR filings, the number of analysts remained the same at 21 persons from 2002 to 2004. To solve this problem, it was necessary to assess significance levels of STRs registered and to deploy manpower according to the assessment results.

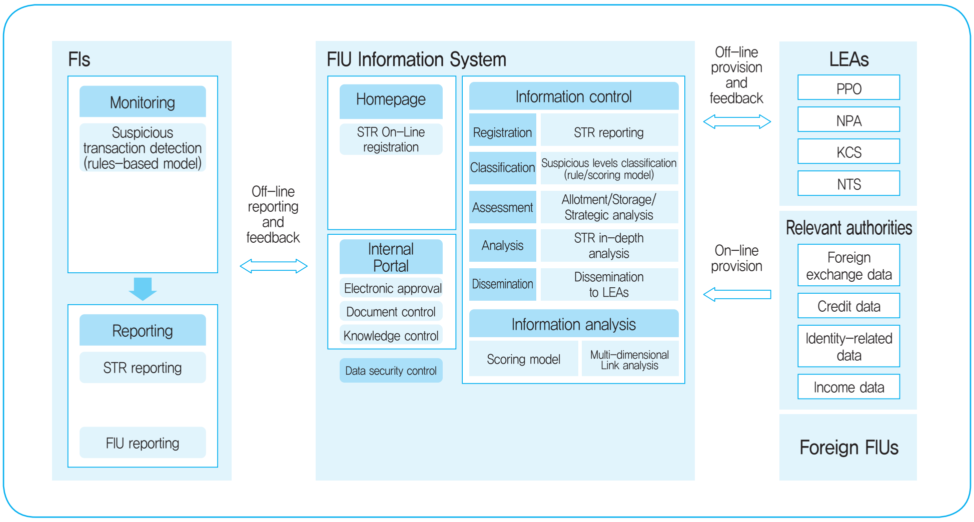
Third, it was necessary to improve the work process. As the First FIU Information Project was focused on building an infrastructure for information collection and analysis, information sharing within KoFIU, information exchange with LEAs and information collection from relevant authorities that was carried out in an inefficient manner.

Finally, KoFIU needed to minimize the work vacuum that resulted from changes in personnel. Analysts of KoFIU come from relevant authorities including the Public Prosecutors' Office (PPO), National Tax Service (NTS), Korea Customs Service (KCS), etc. to secure expertise for each field. So, whenever there was a change of personnel, a work vacuum was inevitable.

2.2.2. Implementation Details

The scope of the Second FIU Information Project is to build an on-line STR reporting system, to transfer and improve KoFIU's homepage, to improve work processes such as electronic approval, to build an infrastructure for the Knowledge Management System (KMS), and to set up a security control system corresponding to online environments. The composition of the FIU system is set out in [Figure 3-4].

Figure 3-4 | Composition of the FIU Information System of the Second Project



Source: Korea Financial Intelligence Unit

a. On-line STR Reporting System

The paper-based registration system based on the standardized STR program distributed to FIs was replaced with an online reporting system. Reporting form and method as well as registration feedback were developed after a series of discussions with FIs.

a) Reporting Form

The reporting form, developed in the first project and distributed to FIs in disk format, was revised to be suitable for the online reporting system. Also, the customer-based reporting system was changed to the case-based one, and the number of attached documents, required when STR is filed online, was dramatically reduced, with the contents of attached documents included in the reporting form.

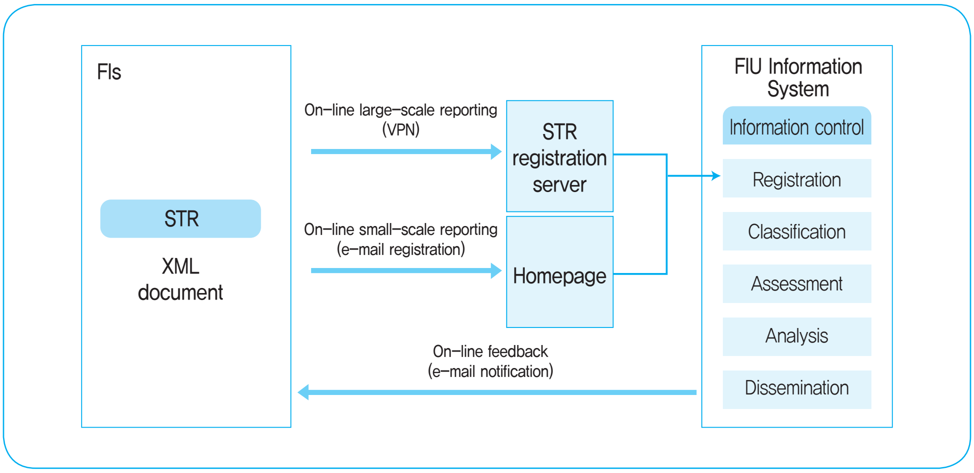
b) Reporting Method

The online reporting system was divided into VPN registration and e-mail registration depending on the volume of STRs. Banks with lots of STR cases were encouraged to register via VPN, while non-banking financial institutions were induced to register via e-mails case by case.

c) Registration Feedback

In order to provide feedback on registration to about 6,000 FIs, the second project built a mailing system to automatically notify registration results via e-mails. In addition, it enhanced the automatic search function of the analysis system to provide convenience to analysts. The flow of STR registration and feedback is set out in [Figure 3-5].

Figure 3-5 | Flow Chart of STR Registration and Feedback

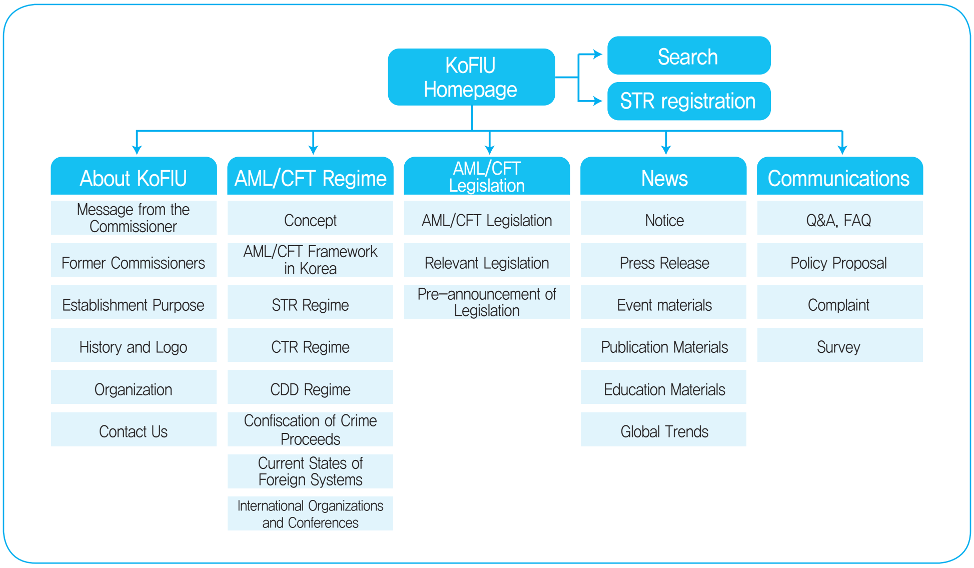


Source: Korea Financial Intelligence Unit

b. Transfer and Improvement of Homepage

The homepage developed during the first project was aimed at simply promoting the newly-adopted AML system. In the second project, the homepage was transferred to KoFIU, with functions such as online reporting system, educating the general public, collection of public opinion, communication activities, etc. were greatly improved. The composition of the homepage is shown in [Figure 3-6].

Figure 3-6 | Composition of KoFIU's Homepage



Source: Korea Financial Intelligence Unit

c. Improvement of Work Processes including Electronic Approval, etc.

Work process improvement efforts in the second project consist of building an internal portal site, improving the information control process, establishing an online interface with relevant authorities, and setting up a statistics calculation system.

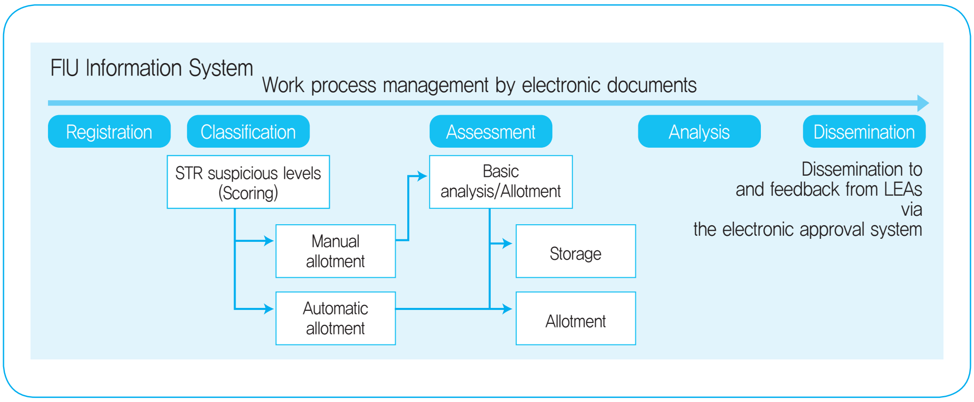
a) Establishment of an Internal Portal Site

The internal portal system, serving as a gateway to all unit systems, was set up to enhance the interface between existing and new unit systems such as information control, information analysis, electronic approval and knowledge management, along with reinforcing system security including user authentication. In addition to these, the internal portal system provides a community function for information sharing within KoFIU, relevant laws provision function, and e-mail function.

b) Improvement of Information Control Process

The most striking change in the information control process was the adoption of the scoring model. When a STR is filed from FIs, its suspicious level is automatically scored. And the case is automatically allocated to analysts if its suspicious level is high, while the case is stored without further analysis if its suspicious level is low, which contributed to raising efficiency of work processes. Assessment and analysis process using scoring technology is shown in [Figure 3-7].

Figure 3-7 | Assessment and Analysis Process Utilizing Scoring Technology



Source: Korea Financial Intelligence Unit

In order to establish the scoring model, the second project categorized types of suspicious transactions by analyzing STRs, and quantified suspicious levels by adding weighted values to various parameters such as transaction amount, frequency, etc. One of the major characteristics of the Second FIU Information Project is to provide scoring technology so that suspicious levels of foreign exchange and suspicious transactions can be measured. The scoring model comprises rules-based foreign exchange, data-mining foreign exchange and STR suspiciousness score. Rules-based and data-mining foreign exchange offer suspiciousness scores on foreign exchange transactions, while STR provides them on STR. Also, the second project introduced the electronic approval system to make up for the lack of information system with LEAs.

c) On-line Interface with Relevant Authorities

In the first project, financial transactions and credit data necessary for assessment/analysis of STR were transferred in paper form, which was inefficient and not secure. In order to tackle these problems, in the second project, KoFIU carried out an 'online interface with relevant authorities'. For this, KoFIU had a series of meetings with relevant authorities such as the Bank of Korea (BOK) and the Korea Customs Service (KCS). In short, KoFIU receives information from relevant authorities online or via e-mails, the electronic approval system, etc. and then puts the information into its database for analysts' timely use.

d) Statistics Calculation System

The statistics calculation system was built to help analysts calculate and search in various dimensions (customer, analyst, assessor, etc.) STRs filed by FIs, credit and foreign exchange data obtained from relevant authorities, and information controlled by the information control system.

d. Establishment of Infrastructure for the Knowledge Management System

The quality of STR assessment and analysis is largely decided by experiences, judgment and know-how of each analyst.

KoFIU comprises AML/CFT experts from LEAs[4] responsible for the investigation and decision on predicate offences for ML and financing for offences of public intimidation.[5] This staffing method can secure expertise in analyzing suspicious transactions in various dimensions, but there is a shortcoming—not being able to pass down analysts' knowledge and know-how when there is a change in personnel. In order to overcome this problem, the second project established the Knowledge Management System (KMS), in which analysts not only share tangible or intangible knowledge they accumulated in the assessment and analysis processes but also make a rational decision based on the information. The key functions of the KMS are knowledge writing/registration/revision (knowledge accumulation activities), knowledge search/inquiry/reading request (knowledge utilization activities), user assessment, selection of superior knowledge, and an individual map. (knowledge vitalization activities).

e. Establishment of a Security Control System Corresponding to Online Environments

With the adoption of an online STR reporting system, networks became vulnerable to security threats. To tackle this problem, security measures were established such as document encoding, de-militarized zone (DMZ), and server security, as shown in <Table 3-3>.

Table 3-3 | Security Measures

Achievement	Content
Utilization of GVPN when reporting massive number of STRs	• When FIs access the STR registration server to report STRs, they can access via the Government Virtual Private Network (GVPN) of the Ministry of Government Administration and Home Affairs (MGAHA) after being authenticated through GVPN Client
DMZ & intrusion detection system	• Secure DMZ between external and internal networks by adding an additional intrusion detection system in order to block direct outside access • The intrusion detection system can detect illegal intrusion via network
Online document security	• Secure confidentiality of documents by applying multiple encoding/descrambling technologies
Server security	• Carry out user-based access control to main DB servers, and prevent/detect illegal intrusion by adopting security OS

Source: Korea Financial Intelligence Unit

4. PPO, NPA, NTS, KCS, etc.

5. Fraud, bribery, illegal tax refund, illegal flight of foreign currency, etc.

2.2.3. Achievements of System Establishment

The Second FIU Information Project not only improved the efficiency of assessment and analysis processes by making all information flows online among FIs, KoFIU and relevant authorities, but also helped analysts share information to make reasonable decisions. The major achievements of the project can be summarized as follows.

a. Online Registration/Analysis/Dissemination of Financial Transaction Information

The Second FIU Information Project, called the “Clean Desk Project,” built an electronic report system in which STR registration, analysis and dissemination were all carried out online from December 1, 2004. Also, information collection and search, approval of analysis reports and dissemination to LEAs were all implemented in the form of electronic documents.

In short, an old work process characterized by paper and mailings was changed into a new one characterized by electronic documents and the Internet. This change not only accelerated the speed of information transfer but also raised work efficiency. As shown in <Table 3-4>, the total number of STRs filed by FIs using the standardized STR program from 2001 to 2004 stood at 6,699, but the number more than doubled to 13, 459 in 2005 alone with the introduction of the online system. And since then, the number has steadily been rising about 2.5 fold every year. In addition, thanks to the online reporting system and the active promotion on the STR regime, banks’ STR filing rate, as shown in [Figure 3-8], rose from 88.36% in 2002 to 97.82% in 2007. Meanwhile, STR filings from non-banking financial institutions are significantly lower compared to those from banks, but in fact, they also greatly increased after the adoption of the online reporting system in 2005. The online reporting system expanded the STR filing trend to non-banking financial institutions such as securities and insurance companies.

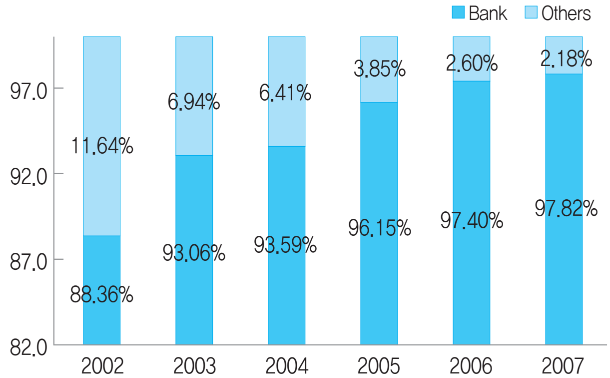
Table 3-4 | The Number of STR Filings by FI from 2002 to 2007

(Unit: case)

Classification	Bank	Securities	Insurance	Others	Total
2002	243	30	-	2	275
2003	1,623	101	6	14	1,744
2004	4,380	225	9	66	4,680
2005	12,941	260	51	207	13,459
2006	23,522	199	58	370	24,149
2007	51,330	218	56	870	52,474

Source: KoFIU

Figure 3-8 | The Rates of STR Filings by Financial Institution



Source: KoFIU

b. Improvement of Allotment Process

STRs significantly grew in quantity, but lagged far behind in quality. In other words, financial transactions with low suspicious levels were often reported. The system, set up in the first project, conducted in-depth analysis on all reported STRs, which in turn severely lowered work efficiency. So as to prevent a decline in work efficiency and conduct the so-called 'selection and concentration' approach on analysis process, the scoring technology was adopted. The improvement of the allocation process using the scoring technology enabled analysts to focus on STRs with higher suspicious levels, thereby enhancing work efficiency. Also, the scoring model made it possible to assess the quality of STRs filed by FIs.

<Table 3-5> shows that the ratio of in-depth analysis to STRs filed to KoFIU was 75.6% (2002), 71.8% (2003) and 91.1% (2004), or an average of around 85.4%. However, the ratio of dissemination to analysis was 50% (2002), 34.5% (2003) and 23.3% (2004), or a mere 26.7% on average. This represents that the STR system entered into stability from the quantitative aspect, but did not in a qualitative aspect. But after applying the scoring model in the second project, the ratio of in-depth analysis to STRs plummeted by more than 50% in 2005 compared to the previous year, while the dissemination ratio to LEAs went up by more than 30% in the same year. Thanks to this increased efficiency, KoFIU could deal with a sharp rise in STR filings without additional recruitment.

Table 3-5 | The Rates of STR Registration, Analysis and Dissemination by Year

(Unit: case)

Classification	2002	2003	2004	2005	Total
No. of STRs (A)	275	1,744	4,690	13,459	20,167
No. of In-depth Analysis (B)	208	1,252	4,272	5,846	11,578
Ratio of In-depth Analysis to STRs (B/A)	75.6%	71.8%	91.1%	43.4%	57.4%
No. of Disseminated STRs (C)	104	432	994	1,799	3,329
Ratio of Dissemination to Analysis (C/B)	50.0%	34.5%	23.3%	30.8%	28.8%

Source: KoFIU

c. Establishment of Infrastructure for Information Sharing through Documentation and Database

KoFIU comprises AML/CFT experts from the Public Prosecutors' Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), among other organizations, so their expertise, knowledge and know-how disappeared when there was a change of personnel, not accumulated as the knowledge of KoFIU. In order to overcome this problem, KoFIU had exerted various efforts to build a database for analysis techniques since its founding. One of them was to publish casebooks, and another was to build the KMS.

In terms of casebooks, representative cases, which are completed from registration, analysis and dissemination of STR to further investigation and indictment, are documented by types of predicate offences. Cases included in casebooks are uploaded and controlled in KoFIS so that the content is searched and analyzed anytime.

Also, the Knowledge Management System helps analysts share their accumulated knowledge and know-how by registering them on the system. Further, KoFIU encouraged analysts to share their experiences and know-how by providing incentives to those who registered the most.

2.2.4. Improvements

Although the Second FIU Information Project built an on-line system for information collection, analysis and dissemination, there was a limit in fully dealing with the rapidly rising STR filings with limited manpower. Improvements derived from the second project are as follows.

a. Increase in the Number of Analysis Cases per Analyst due to Rising STRs

As shown in <Table 3-6>, the number of analysis cases per analyst stood at just 10 in 2002 and 60 in 2003. But the number exploded to 203, up by more than 300%, in 2004 with a sharp rise in STR filings. In 2005, the ratio of in-depth analysis against STRs declined to 43.4% with the adoption of the scoring technology, but due to limited manpower, the number of analysis cases per analyst climbed to 278 cases, up about 40% from the last year. Therefore, it was necessary to build a system that can flexibly respond to the rapidly rising STRs with reference to the cases of advanced countries.

Table 3-6 | The Number of In-depth Analysis per Analyst by Year

Classification	2002	2003	2004	2005
No. of STRs	275	1,744	4,680	13,459
No. of In-depth Analysis (A)	208	1,252	4,272	5,846
No. of Stored Cases	67	492	408	7,613
Ratio of Storage to STRs	24.36%	28.21%	8.72%	56.56%
Ratio of In-depth Analysis to STRs	75.64%	71.79%	91.28%	43.33%
No. of Analysts	21	21	21	21
No. of In-depth Analysis per Analyst	10	60	203	278

Source: KoFIU

b. Necessity of Building Communication Channels with FIs and LEAs

The online system was built for effective information collection from FIs and dissemination to LEAs, but mutual communication channels among FIs, KoFIU and LEAs were not sufficient. As the quality of STRs deteriorated, it was necessary to build a system that gives feedback on STRs to FIs. In addition, there was no system to accumulate measures taken by LEAs and to utilize them in analysis, making it difficult for KoFIU to improve the accuracy of analysis.

c. Necessity to Accumulate Data by Financial Product and Crime Type

STR reporting process, or registration → basic analysis → review → allocation → in-depth analysis → decision → dissemination, was computerized, but there was no accumulated data by financial product and type of crime.

d. Improvement of the Strategic Analysis System to Respond to Rising Stored Cases

From 2002 to 2004, the ratio of stored STRs to STR filings remained below 28%, but with the adoption of the scoring model in 2005, the ratio rose to 56.56%, a two-fold increase. From the perspective of each case, they could be classified as stored cases because of their low suspicious levels, but when they are analyzed comprehensively, they can result in meaningful results. Therefore, the need to improve the strategic analysis system emerged.

2.3. The Third Project (Intelligence): CTR Analysis and Sophistication of Analysis Work

2.3.1. Purpose of Establishment

With the introduction of the CTR regime in January 2006, the Third FIU Information Project aimed to establish an effective CTR information collection and analysis system. Also, the expansion of electronic finance and diversification of financial products brought about an evolution of ML techniques, which in turn resulted in the need to advance analysis work. Along with this, in order to raise efficiency in the allocation of human resources, it was necessary to re-design the information control and analysis processes. The core requirements to achieve those goals can be summed up as follows.

First, for the soft landing of CTR system newly adopted in January 2006, it was necessary to provide guidelines defining CTR's reporting threshold, period, data interface method, etc. to FIs, as well as to build an effective information control and analysis system.

Second, the amount of STRs reported to KoFIU skyrocketed from 275 cases in 2002 to 24,149 cases in 2006, or about an 88-fold increase, but the dissemination rate to LEAs fell from 50% in 2002 to 23.3% in 2004. This can be attributed to an increased efficiency of analysis work thanks to the scoring technology adopted in the second project. However, since 2002, the number of STRs rapidly rose by more than 250% every year, so it was necessary to re-engineer information analysis and strategic analysis processes.

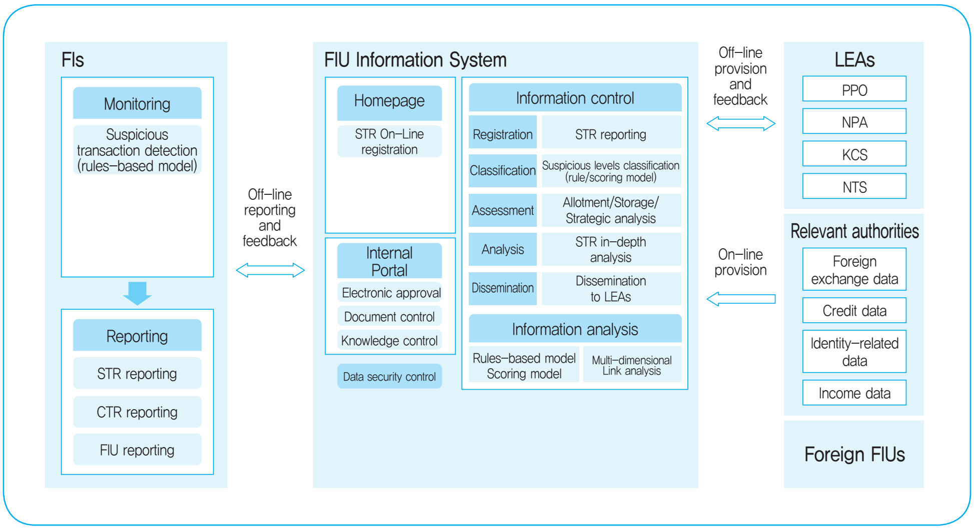
Third, as CTR data and foreign exchange derivatives transaction data were added, there was a growing need to re-organize data and a system for sophistication of strategic analysis.

Finally, in order to help customer due diligence (CDD) procedure introduced in 2006 soft-land together with the CTR system, education and promotion on the new systems were needed.

2.3.2. Implementation Details

The scope of the Third FIU Information Project is to build a CTR reporting system, to advance strategic analysis process, to improve analysis process and to promote the AML system to FIs. The composition of the FIU Information System established in the Third project is set out in [Figure 3-9].

Figure 3-9 | Composition of the FIU Information System of the Third Project



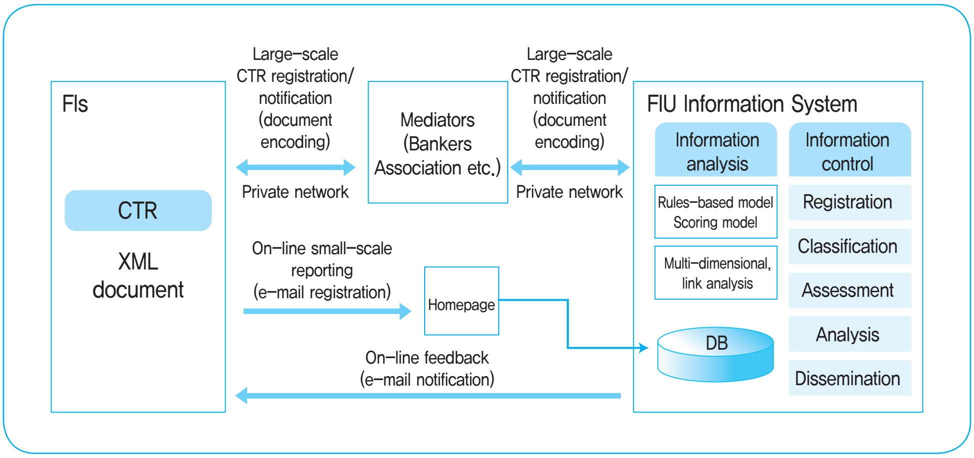
Source: Korea Financial Intelligence Unit

a. Establishment of a CTR Reporting System

KoFIU decided the CTR form through a series of meetings with FIs prior to the development of the CTR system, and distributed this form as well as the data interface format and method to all reporting entities. The major functions of the CTR system are (i) to monitor the status of data transfer when FIs transfer CTR data (monitoring function); (ii) to automatically distribute the interlock module when banks transfer data (automatic module distribution function); and (iii) to automatically apply the interlock module through remote control (automatic module application function).

Also, in order to efficiently receive massive CTR data from about 6,000 FIs, KoFIU designated the KFB and the Securities Dealers Association as mediators, and used their private networks for stable transfer of massive data without any new investments. As for small-sized reporting entities with a few CTR cases, KoFIU had them report directly via the Internet. In addition, up-to-date security technologies, including encryption applied to e-commerce and authentication using electronic signature, were also applied to deal with security problems that could happen while reporting via electronic networks. The flow of CTR registration and feedback is set out in [Figure 3-10].

Figure 3-10 | Flowchart of CTR Registration and Feedback



Source: Korea Financial Intelligence Unit

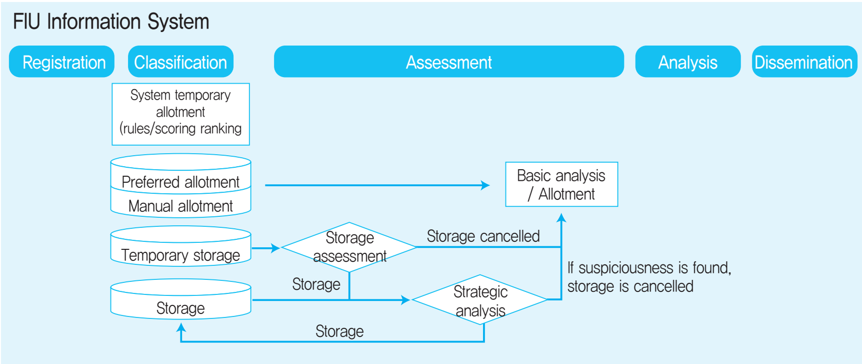
b. Sophistication of the Strategic Analysis System

KoFIU advanced the strategic analysis system by adding functions such as CTR-STR link analysis, foreign exchange derivatives analysis, development of analysis reports that can help figure out foreign exchange trends resulting from capital liberalization, etc. Also, for effective utilization of these link functions and analysis reports, KoFIU conducted cleansing on errors of raw date as well as adding a function with which users can control search ranges according to the purpose of analysis and usage when analyzing existing reports.

c. Improvement of Analysis Process

KoFIU established an intelligent analysis system, which allots STRs automatically using rules-based and scoring technologies. When a STR is filed from FIs, this system calculates its suspicious ranking based on each technology, and calculates the final suspicious ranking combining the two results. Then, analysts decide whether the STR should go through in-depth analysis or not based on the final result. Analysis process using the rules-based and scoring models is shown in [Figure 3-11].

Figure 3-11 | Analysis Process Using Rules-based and Scoring Models



Source: Korea Financial Intelligence Unit

STRs given an above a designated suspicious ranking are automatically assigned to the in-depth analysis stage, thereby saving unnecessary time and efforts of basic analysis. Also, in order to deal with the rising number of STR filings, the system provides an 'intelligent automatic allotment function', which allots STRs comprehensively considering the STR's suspicious level and analyst's availability.

STRs that are judged to have low suspicious levels are stored in the database for later use when necessary. However, some of these STRs could have undetected higher suspicious levels. In order to prevent these STRs from being abandoned without further analysis, KoFIU introduced a 'stored cases assessment system' in the classification stage in which analysts conduct assessment on all stored STR cases to determine which cases need further analysis. Based on assessment results, analysts divide stored STRs into three categories: storage cancellation, strategic storage, and storage. 'Storage cancellation' means embarking on in-depth analysis, 'strategic analysis' indicates no need for in-depth analysis but a need to observe long-term transaction trends and patterns, and 'storage' means storage into KoFIU's database without further analysis. Stored cases with the 'storage' decision can be used as a clue for later STR analysis, or if its relationships with newly-reported STRs are found, and analyzed in-depthly later.

d. Promotion of the AML Regime

For the soft-landing of CDD and CTR systems enforced from January 2006, KoFIU held public hearings in advance to collect opinions from the public and FIs. Also, it ran poster and TV/radio advertisements to promote the systems.

2.3.3. Achievements of System Establishment

The major achievements of the Third FIU Information Project are to successfully establish the newly-adopted CTR regime as well as to build an intelligent analysis system that can effectively cope with rising STR filings.

a. Soft-landing of the CTR Regime

The CTR system was introduced in 2005 in accordance with the "road map for implementation of FATF Recommendations," and its reporting form, regulation and relevant information systems were established for its effective implementation.

As shown in <Table 3-7>, after the enforcement of the CTR system, the amount of CTRs reported to KoFIU in 2007 fell by about 33.56% compared to the amount in 2006 (with report threshold of KRW 50 million), which indicates the soft-landing of the regime. Rapid hikes in 2008 and 2010, as shown in [Figure 3-12], were because the report threshold was gradually lowered to KRW 30 million in 2008 and to KRW 20 million in 2010. Afterwards, currency transactions were on a gradual decline.

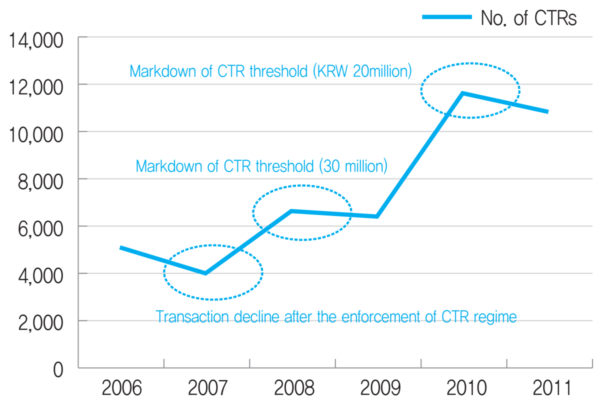
Table 3-7 | The Number and Amount of CTRs by Year

(Unit: thousand, trillion)

Classification	2006	2007	2008	2009	2010	2011
No. of CTRs	5,013	3,875	6,678	6,441	11,606	10,811
Amount of CTRs	149	99	136	133	208	202
Rate of Change in Amount		▼ 33.56%	▲ 37.37%	▼ 2.21%	▲ 56.39%	▼ 2.88%

Source: KoFIU

Figure 3-12 | Development of CTR Amount by Year



Source: Korea Financial Intelligence Unit

b. Raising Assessment and Analysis Efficiency through Process Improvement, etc.

Since the intelligent analysis system using rules-based and scoring technologies was introduced in 2005, the number of STR filings, as shown in <Table 3-8>, went up to 24,149 in 2006, and soared to 329,463 in 2011 (a 24.5-fold hike against 2005). But the ratio of in-depth analysis to STRs fell from 43.44% in 2005 to 27.32% in 2006 (16.12% decline), and to 5.01% in 2011 (a whopping 38.43% decline against 2005). Contrary to the in-depth analysis rate, the dissemination rate to LEAs rose from 30.77% in 2005 to 34.36% in 2006 (3.59% hike), and to 79.48% in 2011 (a whopping 48.71% hike against 2005). All these reflect that the efficiency of assessment and analysis works has greatly improved. In-depth analysis and dissemination rates by year are shown in [Figure 3-13]. In conclusion, KoFIU could raise the dissemination rate against the in-depth analysis rate by concentrating on STRs with relatively higher suspicious levels (so-called ‘selection and concentration’ approach) despite its limited manpower.

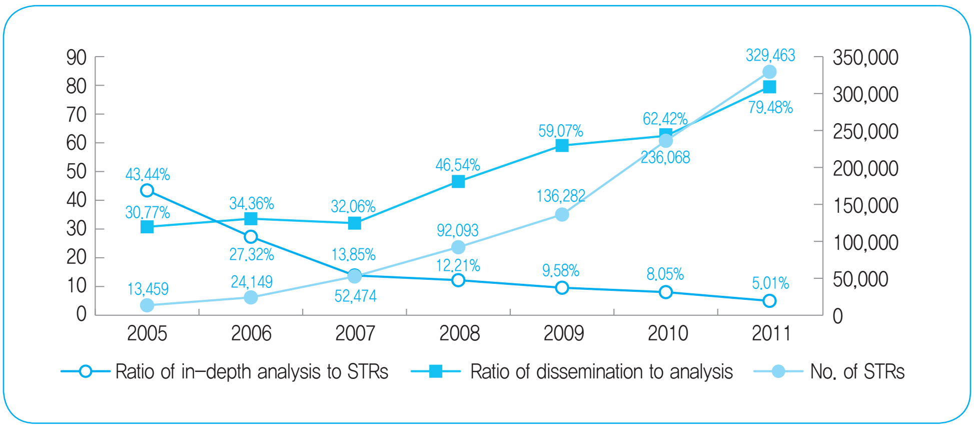
Table 3-8 | STR Registration, Analysis and Dissemination Status by Year

(Unit: case, person)

Classification	2005	2006	2007	2008	2009	2010	2011	Total
No. of STRs	13,459	24,149	52,474	92,093	136,282	236,068	329,463	883,988
No. of In-depth Analysis (A)	5,846	6,598	7,270	11,246	13,053	19,012	16,494	79,519
No. of Stored STRs	7,613	17,551	45,204	80,847	123,229	217,056	312,969	804,469
Storage Rate	56.56%	72.68%	86.15%	87.79%	90.42%	91.95%	94.99%	91.00%
In-depth Analysis Rate	43.44%	27.32%	13.85%	12.21%	9.58%	8.05%	5.01%	9.00%
No. of Analysts	21	21	28	28	27	28	26	179
No. of In-depth Analysis per Analyst	278	314	260	402	483	679	634	3,050
No. of Dissemination to LEAs (B)	1,799	2,267	2,331	5,234	7,711	11,868	13,110	44,320
Dissemination Rate (B/A)	30.77%	34.36%	32.06%	46.54%	59.07%	62.42%	79.48%	55.74%

Source: KoFIU.

Figure 3-13 | Development of STR In-depth Analysis and Dissemination Rates by Year



Source: Korea Financial Intelligence Unit

However, the number of in-depth analysis per analyst climbed from 278 in 2005 to 314 in 2006 (13% hike), and to 634 in 2011 (a staggering 128% hike from 2005), which was the result of the combination of rising STR filings and limited manpower. In order to deal with the heavy workload while securing analysis quality, KoFIU strived to reduce the average analysis period per case through process improvement, etc.

As part of these efforts, KoFIU tried to enhance the analysis capacity of each analyst, provide systematic information via information networks, improve the information collection process of administrative data such as resident registration, crime data, immigration status, etc., and build an individual control system for each analysis period. Also, to reinforce the analysis ability of each analyst, it offered education about analysis techniques, actively shared analysis know-how, reference materials and analysis cases as well as discovered and offered incentives to exemplary analysis cases.

Thanks to these multi-faceted efforts, the average STR registration, analysis and dissemination period was reduced from 55 days in 2004 to 45 days in 2005, and to 32 days in 2008, as shown in <Table 3-9>.

Table 3-9 | Average Analysis Period per Year

(Unit: day)

Classification	2004	2005	2006	2007	2008
Analysis Period per Case	55	45	47	46	32

Source: KoFIU

2.3.4. Improvements

The Third FIU Information Project not only helped the newly-adopted CTR system to be successfully implemented but also greatly improved assessment and the analysis process, but it was limited in building an effective control system for rules and scoring models as well as an effective strategic analysis system on stored cases. Additional improvements derived from the third project are as follows.

a. Necessity to Build a Control System on Rules-based and Scoring Models

In the analysis system based on rules and scoring technologies, which are designed to accumulate and utilize knowledge and know-how, cleansing on data should be constantly carried out to maintain the effectiveness of scores representing risk levels. In addition, at a new environment where new financial products and services are constantly developed as a result of the opening and complications of the financial market, the accuracy of rules-based and scoring technologies should be constantly monitored to promptly respond to changing environments such as advancement of ML techniques, creation of financial products, and expansion of reporting range.

b. Necessity to Establish a Strategic Analysis System

Despite a steady increase in the number of in-depth analysis, the ratio of in-depth analysis to STRs showed a decline, and the storage rate rose. The rise in the storage rate, meaning the rise in the number of stored cases excluded from in-depth analysis, is accompanied by risks. In order to reduce the risk, it was necessary to build a strategic analysis system, which analyzes raw data retained by KoFIU and detects suspicious transactions using OLAP and visual-links tools, together with STR analysis.

As shown in <Table 3-10>, KoFIU conducted strategic analysis on stored STRs from 2003, and analyzed 23.78% of stored cases and disseminated 7.69% of the analyzed cases, or nine cases, in 2003. However, the ratio of analysis cases to stored STRs had sharply plunged since then, standing at 0.06% in 2011, which meant that the change in strategic analysis methods was inevitable. Fortunately, the ratio of dissemination to analysis jumped from 7.69% in 2002 to 75.61% in 2010, and to 51.63% in 2011, as shown in [Figure 3-14]. This was attributable to increased analysis efficiency by enhancing the analysis capability of each analyst.

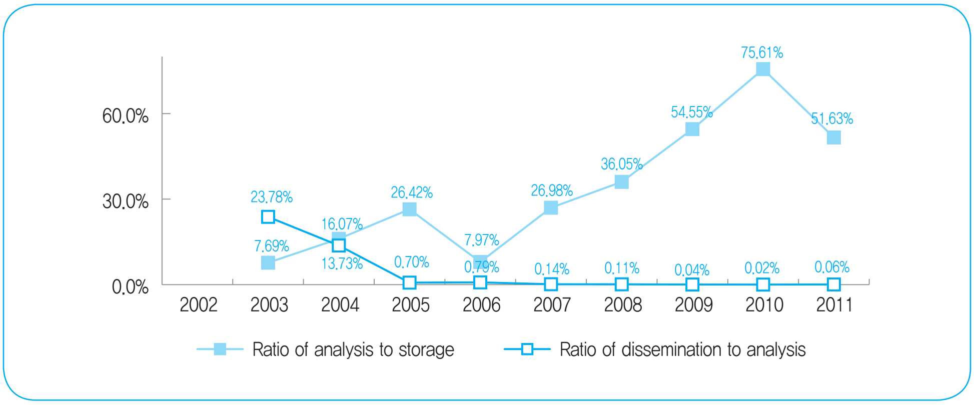
Table 3-10 | The Number of Strategic Analysis and Dissemination Cases by Year

(Unit: case)

Classification	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
No. of Stored Cases	67	492	408	7,613	17,551	45,204	80,847	123,229	217,056	312,969
No. of Analysis Cases	-	117	56	53	138	63	86	44	41	184
No. of Disseminated Cases	-	9	9	14	11	17	31	24	31	95
Ratio of Analysis to Storage	-	23.78%	13.73%	0.70%	0.79%	0.14%	0.11%	0.04%	0.02%	0.06%
Ratio of Dissemination to Analysis	-	7.69%	16.07%	26.42%	7.97%	26.98%	36.05%	54.55%	75.61%	51.63%

Source: KoFIU.

Figure 3-14 | Development of Strategic Analysis and Dissemination Cases per Year



Source: Korea Financial Intelligence Unit

For establishment of the effective strategic analysis system, it is necessary to support human resources, process (scenario), and the system.

a) Human Resources

FinCEN based in the US has around 300 regular staff and 20% of them, or 60 persons, are placed in the Analytics Division to carry out strategic analysis, while KoFIU placed only 2 persons out of its 26 staff to strategic analysis work as of 2011. In this regard, it was crucial to increase the number of analysts to facilitate strategic analysis work.

b) Process (Scenario)

Scenarios related to foreign exchange data analysis were established relatively well by plenty of experts, but its reliability was low due to the lack of empirical evidence. Also, as the selection of scenarios was largely determined by analysts' subjective experiences, knowledge and observations, the scope of analysis was likely too narrow. So, it was necessary to establish an objective standard and methods for scenarios selection.

c) Knowledge Management

To build an effective strategic analysis system, it was necessary to systematically arrange and standardize knowledge necessary for strategic analysis processes and to compose detailed manuals for each process. Also, along with the standardization of knowledge, a knowledge sharing system should be built in which analysts' experiences and know-how are systematically accumulated, controlled and shared with one another.

d) System

The strategic analysis is an analysis method to select STRs to be analyzed based on a variety of basic data retained by KoFIU, not based on the data of each STR. And this requires a computer with massive capacity. Therefore, it was essential to secure enough capacity to carry out strategic analysis. In addition, strategic analysis scenarios verified through assessment and analysis should be regularly monitored.

c. Necessity for Integrated Management of Analysis Tools

Analysis tools such as rules-based and scoring technologies and visual links were then used individually in each stage of registration, basic analysis, allotment, appointment and in-depth analysis, but it was hard and inconvenient to check each result. Therefore, it was necessary to assist these tools to be used in an integrative way, thereby creating a synergy effect and raising utilization rates of the tools.

d. Necessity of STR Form Improvement and Registration Data Cleansing

The FIU Information Project made STR filing more convenient through the online reporting system, but due to the complexity of the STR report form and the difference of customer data retained by each FI, STRs included a lot of useless data. As a result, when conducting analysis based on these data, additional data requests were needed to correct them, which, in turn, lengthened the analysis period as well as lowered work efficiency. To address this problem, it was necessary to improve the STR form, strengthen input control to prevent input errors, and verify the accuracy and appropriateness of data in the registration stage.

2.4. The Fourth Project (Feedback): Establishment of a Comprehensive AML Portal Site

2.4.1. Purpose of Establishment

The fourth FIU Information Project aimed to verify the effectiveness of the rules-based analysis system developed in the third project, improve the database for integrative data search, establish an information security system for information accumulated in the database and build an effective network for two-way communications with relevant organizations including FIs. The key requirements of the project can be summarized as follows.

First, KoFIU provided the infrastructure for information control and analysis through the FIU Information System and thus contributed to raising the efficiency of analysis work, but the one-way reporting and analysis system from FIs to KoFIU hampered its active response to the rapidly changing external and internal environments. Accordingly, the need to build a comprehensive portal site equipped with a bilateral communications feature surfaced. To this end, KoFIU had to overhaul the STR reporting program developed for FIs and extend the system to LEAs as well as build data sharing channels between reporting entities and analysts so that analysts can collect necessary information promptly until the completion of analysis. This not only shortened analysis and dissemination periods but also improved the quality of STR by checking input errors in real time.

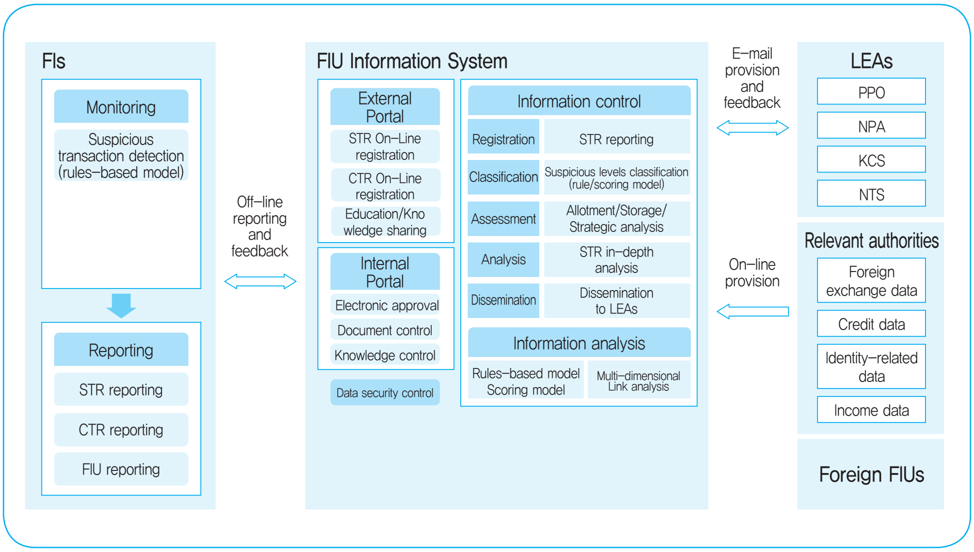
Second, in order to effectively respond to the rapidly changing financial environments, it was necessary to advance assessment and analysis systems. For this, KoFIU had to add rules considering the characteristics of financial products and fields, consistently verify the effectiveness of rules-based and scoring models through appropriateness evaluation, etc., and improve the database to raise the efficiency of analysis work.

Finally, KoFIU needed to build an information assets management system for effective control of accumulated data as well as an information security system across KoFIU's all information systems. By adopting the information technology architecture (ITA), KoFIU had to structurally design KoFIU's businesses, information, application system, security support technology, etc. and present a blueprint illustrating the relationships of these factors.

2.4.2 Implementation Details

The scope of the fourth FIU Information Project is to establish a knowledge-based AML portal system, advance analysis system and build information assets management and security systems. The composition of the information system established in the fourth project is shown in [Figure 3-15].

Figure 3-15 | Composition of the FIU Information System of the Fourth Project

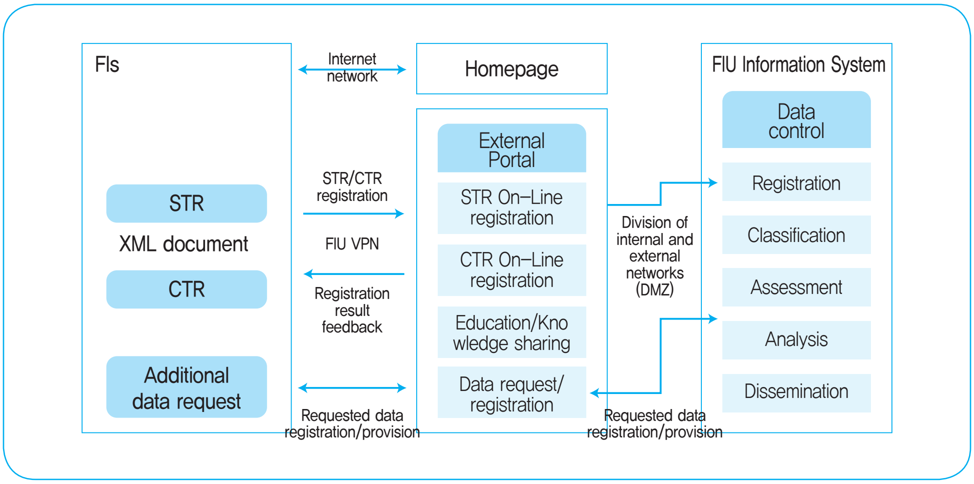


Source: Korea Financial Intelligence Unit

a. Establishment of a Knowledge-based AML Portal System

In order for FIs to fill in the STR form more quickly and accurately through the knowledge-based AML portal system, KoFIU improved the standardized STR program, reporting procedures and systems of reporting entities. Also, it unified reporting channels to the KoFIU VPN, instead through e-mail or GVPN of the Ministry of Public Administration and Security (MOPAS), making it possible to check the transferring state in real time. Additionally, KoFIU not only reinforced security on notices, AML-related materials, and statistics, but also built a bilateral communications system between analysts and reporting entities, making it possible for analysts to ask questions or request additional information in the in-depth analysis stage. The composition of the portal system is set out in [Figure 3-16].

Figure 3-16 | Composition of Knowledge-based AML Portal System



Source: Korea Financial Intelligence Unit

b. Advancement of Assessment and Analysis Systems in line with Rapidly Changing Financial Environments

The FIU Information System had a dual database system, or information control system and information analysis system, to effectively control date between the two systems. Because of this, it was difficult to conduct a comprehensive search on the suspect about information such as suspicious transaction information, previous reports, identity data, and foreign exchange data, among others. To overcome this shortcoming, KoFIU established a suspect-based analysis system to help analysts figure out transactions conducted by an identical person under different identification numbers.[6] Also, it analyzed data accumulated for one year using the data mining technique, and based on the results, re-set suspiciousness parameters of rules and scoring models.

c. Establishment of Information Asset Management and Security Systems

In order to effectively control information assets, KoFIU built an information asset management system, called information technology architecture (ITA), which categorizes information into KoFIU's business, data, applications, and technology and security elements in an objective manner and builds control systems for them. In addition, KoFIU established an information security system for the stable operation of the comprehensive AML portal system, along with carrying out a security diagnosis on information systems (server, network, etc.) and web applications.

6. Resident registration number, passport number, business license number, etc.

2.4.3. Achievements of System Establishment

The Fourth FIU Information Project yielded an effective bilateral communications network between KoFIU and FIs.

By improving the existing FIU Information System, KoFIU established a bilateral, comprehensive portal system, greatly increasing the speed of information flows between KoFIU and reporting entities. Also, in order to build a FI-centered AML regime, KoFIU improved the functions of the standardized STR program, and thus improved the user's convenience and work efficiency. In fact, STR input items increased, but input time reduced, showing increased efficiency of reporting and analysis. In particular, it improved the quality of STRs by offering through the comprehensive portal system error information in real time as well as feedback such as various statistics to reporting entities.

2.4.4. Improvements

The Fourth FIU Information Project not only enhanced information networks among relevant entities but also improved the quality of STR by checking the appropriateness of data, but there was a limit in improving the effective quality of STR due to legal constraints. Also, information provision to and feedback from LEAs were still operated in an inefficient way.

a. Improvement of STR Quality

In order to improve STR quality, the quality of both data and report content should be improved. The quality of data was relatively improved with the establishment of the comprehensive portal system, but the quality of report content remained the same.

For the improvement of report content, giving reporting entities feedback such as results and follow-up measures on STRs was most significant, but due to legal constraints, individual feedback was impossible. So, KoFIU not only published annual STR case books FIs can refer to when reporting STR but also offered relevant statistics, thereby giving indirect feedback.

Also, consistent monitoring and feedback on transaction monitoring scenarios of FIs was another important way to improve the quality of report content. As the information contained in STR is full and accurate, assessment and analysis works become efficient and KoFIU provides more useful information to LEAs.

b. Improvement of Information Dissemination and Feedback Procedures with LEAs

Information collection from and feedbacks to FIs were all conducted in real time through the comprehensive AML portal system, but communications with LEAs, including information request and dissemination as well as feedbacks on disseminated STRs, were all processed manually in the form of electronic documents. This was because of lack of communication with LEAs on the processes in advance. Also, until then, KoFIU had not focused on improving information flows with LEAs, compared to its efforts to improve the flows with FIs.

Feedback information from LEAs can be utilized as a means to verify the accuracy of each analysis. As shown in <Table 3-11>, a total of 45,851 STRs were disseminated to LEAs as of end of 2011, but only 22,958 cases, or around 50%, were given feedback, while the remaining 22,893 cases received no feedback. Cases with no feedback turned out to be under investigation or completed without any feedback. Consequently, it was necessary to establish feedback procedures for effective information exchange with LEAs.

Table 3-11 | Feedback Status with LEAs

(Unit: case)

Classification	Dissemination	Feedback given				No feedback ****	Rate of no feedback
		Total	Active*	Medium**	Passive ***		
PPO	6,466	3,920	1,308	458	2,154	2,546	39.38%
NPA	11,085	2,809	886	376	1,547	8,276	74.66%
NTS	22,178	12,249	6,889	4,061	1,299	9,929	44.77%
KCS	5,630	3,803	1,798	99	1,906	1,827	32.45%
FSC	481	167	59	5	103	314	65.28%
NEC	11	10	1	9	0	1	9.09%
Total	45,851	22,958	10,941	5,008	7,009	22,893	49.93%

Source: KoFIU

* Active: indictment (PPO), forwarding of indictment suggestion (NPA), accusation/penalty (NTS), etc.

** Medium: suspension of indictment (PPO), suspension of internal investigation (PPO, NPA), utilization of accumulated data (NTS), etc.

*** Passive: freedom from suspicion, suspension of booking (PPO), no right of arraignment (PPO), termination of internal investigation (NPA), etc.

**** No feedback: under investigation or no feedback on completed cases

2.5. The Fifth Project (Optimization): Establishment of an Integrated AML Information Analysis Network

2.5.1. Purpose of Establishment

Until now, the FIU Information Projects not only built infrastructure for systematic information control and efficient information analysis but also focused on actively responding to the development of new financial products and the evolution of ML techniques. However, as the introduction of new systems such as the Enhanced CDD system was expected to induce an explosive number of STR filings, the fifth FIU Information Project aimed to upgrade the existing information analysis system, thus improving information flows along with business processes. The key requirements of this project can be summed up as follows.

First, with system improvements such as the Enhanced CDD, expanding AML duty to the casino sector, enforcement of the Prohibition of Financing for Offences of Public Intimidation Act, expanding the scope of predicate offences for ML (tax evasion), KoFIU needed to improve the existing FIU Information System. Also, in order to help new systems take root and FIs play its role as the outpost for the AML efforts, KoFIU had to provide guidelines for Enhanced CDD and anti-terrorist financing. Enhanced CDD is a system for FIs to assess risk levels of their customers, and based on the results, to apply differentiated CDD measures, which was one of the key recommendations of the FATF. As for casino operators, KoFIU imposed AML duty such as STR, CTR and CDD, considering their business environments.

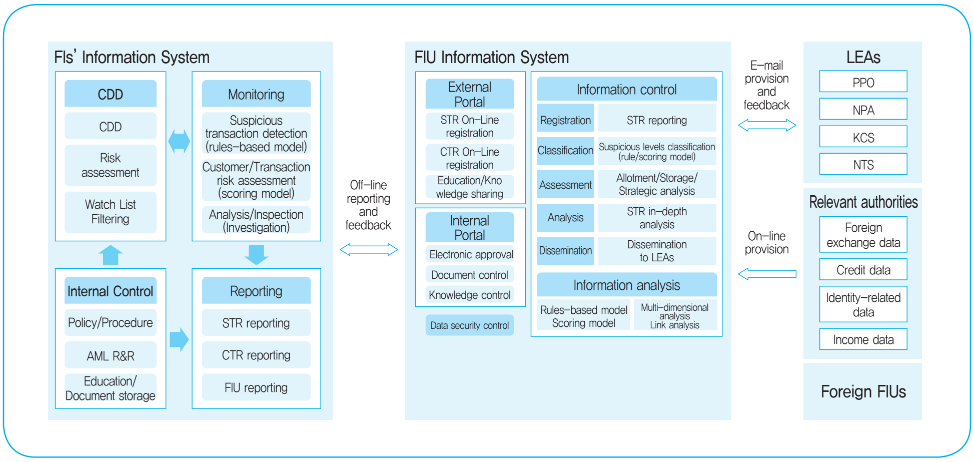
Second, the intelligent analysis system measures its suspicious level when an STR is filed, using rules and scoring models, and selects the STR with a high suspicious level as a subject of in-depth analysis. To increase the accuracy of this system, it was crucial to consistently monitor the system and based on the results, automatically re-set weighted values, etc.

Third, link analysis used in the information analysis system, which analyzed STRs and CTRs related to the suspect, was insufficient in figuring out comprehensive capital flows, so it was necessary to improve the system. Also, KoFIU needed to raise analysis efficiency by re-designing existing analysis processes and collecting more information necessary in the assessment and analysis stages from relevant authorities.

2.5.2. Implementation Details

The scope of the Fifth FIU Information Project is to expand the FIU system in line with institutional improvements, to advance the intelligent analysis system, to build an integrated link analysis system, to raise the efficiency of assessment and analysis process through the business process management (BPM), and to expand the database for assessment and analysis. The composition of the FIU Information System developed in the Fifth project is shown in [Figure 3-17].

Figure 3-17 | Composition of the FIU Information System of the Fifth Project



Source: Korea Financial Intelligence Unit

a. Expansion of System in line with Institutional Improvements

With the implementation of the Enhanced CDD procedure, KoFIU established a dual analysis system to build a comprehensive information analysis network. In this system, first of all, FIs extract suspicious transactions through their own monitoring systems and conduct analysis, and then report to KoFIU STRs with high suspicious levels. For this, KoFIU organized and operated a 'TF Team for Enhanced CDD' in collaboration with FIs for one year. This team drew up business requirements for the implementation of FATF Recommendations, and prepared guidelines for each requirement referring to operating experiences of advanced countries. Also, KoFIU established differentiated risk classification methods according to the types of customers and transactions, provided re-design criteria for CDD procedures, improved STR and CTR electronic report forms, etc., thus helping FIs build their own monitoring systems. It also provided a data interface format and method for interface with the FIU Information System. Meanwhile, as casino operators were included in the list of reporting entities, KoFIU developed STR/CTR electronic reporting forms suitable for the casino sector as well as built the reporting network for them. In addition, in line with the enactment of the Prohibition of Financing for Offences of Public Intimidation Act, it improved the system that detects terrorist financing.

b. Sophistication of the Intelligent Analysis System

As the number of STRs filed by FIs sharply rose, KoFIU elaborated the rules and scoring models in order to raise their hit rates in the registration and classification stages. For the scoring model, KoFIU conducted cleansing on STR-related customers and transaction data.[7] As for the rules-based model, it re-set risk levels of less-used suspicious transaction types and of rules whose dissemination rates to LEAs were low. In addition to these, KoFIU applied an artificial intelligence technique (optimization technique). This technique helped analysis results in the basic analysis and allotment stages by correctly reflecting the rules/scoring models, thus maintaining the reliability of suspicious levels offered by the intelligent analysis system. This artificial intelligence technique also automatically re-set weighted values of each element by learning.

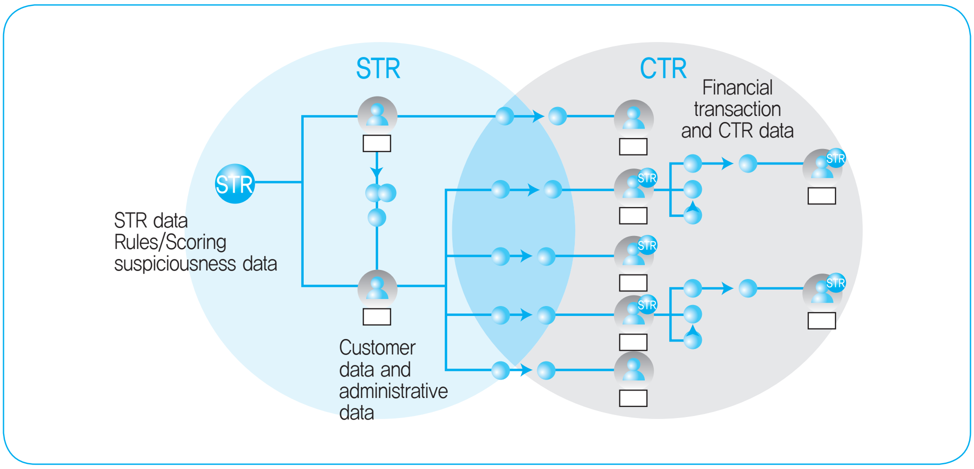
c. Establishment of an Integrated Link Analysis System

The then analysis system included various functions such as multi-dimensional analysis, but did not offer a function to analyze account transaction information attached by FIs when STRs are filed. Considering that more than half of the time was spent on the analysis of account transaction information in in-depth analysis, it was crucial to build a system to analyze the information. But the problem was that FIs were submitting their information in various file formats (excel, Text, PDF, etc.), making it difficult to standardize the data format. To resolve this problem, KoFIU developed a standard form when changing the STR reporting form in 2007, and built a database for account transaction information based on that. Also, by displaying this information in diagram form, KoFIU made it possible for analysts to easily understand the flows of financial transactions. In short, the improved analysis system not only helped understand capital flows by displaying them in diagram form and time order, but also enhanced information utilization by linking STR-related accounts to existing data. Accordingly, the improved analysis system assisted analysts in understanding financial transaction flows of the suspect and the people concerned, making it easier to identify and analyze ML activities.

Furthermore, KoFIU developed an integrated link analysis system. This system made it possible for analysts to comprehensively analyze relationships of existing STR, foreign exchange data, CTR, etc. on one screen. The concept map of the integrated link analysis is set out in [Figure 3-18]. Through this system, analysts were able to detect complicated transaction relations as well as dispersed crime patterns, which were hard to spot in the previous system.

7. Credit status, transaction means, etc.

Figure 3-18 | Concept Map of the Integrated Link Analysis



Source: Korea Financial Intelligence Unit

The integrated analysis system is a support system which helps analysts integrate various analysis tools such as rules and scoring technologies and link analysis, and apply them across all analysis processes. This system provided for visual link information, the results of scoring and rules models (suspicious level and crime types), etc., thus raising analysis efficiency.

d. Raising the Efficiency of Assessment and Analysis Process through BPM

By adopting the business process management (BPM), KoFIU automated simple/ repetitive works and re-engineered the assessment and analysis process in order to make it more adaptable to changing institutions and environments. Through this effort, KoFIU achieved process improvements such as data integration, standardization of input data, standardization of analysis process, analysis progress indication, performance measurement and constant monitoring of the analysis process.

e. Expansion of Assessment and Analysis Database

KoFIU established a database for information that had been requested and controlled in paper form before, increasing the timely use of data. It also changed the offline collection system of additional information, which took much of in-depth analysis period into the online system. In addition, for information exchange with MOPAS (family register data), NTS (tax information), the Supreme Court (family register data), KCS (clearance data), MOJ (immigration data) and others (health and unemployment insurance data, etc.), it defined the data format, data provision methods, etc. in collaboration with them. Then, it received data online and built a database for this information for analysts to use in a timely manner.

2.5.3. Achievements of System Establishment

The major achievements of the Fifth FIU Information Project are (i) to successfully establish newly-adopted systems such as the Enhanced CDD, expand the scope of STR (terrorist financing, tax evasion, etc.) and expand the scope of reporting entities (casino, etc.); and (ii) to advance the assessment and analysis systems by optimizing rules/scoring models, expanding information exchange with LEAs and building an integrated link analysis system

a. Building Infrastructure for FI's AML Information Systems

With the implementation of the Enhanced CDD, all FIs were obligated to comply with the AML regime from December 2008, but AML enforcement requirements and guidelines were not set up yet. Therefore, the Fifth FIU Information Project organized TF teams by industry (bank, securities, insurance, etc.) and composed AML enforcement guidelines through a yearlong consultation with reporting entities and then distributed them. The local AML enforcement guidelines classified their AML activities into customer identification, transaction monitoring and internal control, and specified detailed requirements for each category. Also, in order to help FIs establish their own monitoring systems, KoFIU provided a data interface format and method for interfacing with the FIU Information System.

Korea's AML/CFT framework was not phased in by industry but applied en bloc after a one year grace period. Because of this, there was concern that FIs would be confused. However, KoFIU consulted with them for about one year, offered concrete guidelines for them to comply with, and promoted actively the new system through promotion, education and briefing sessions, thus minimizing confusion and successfully establishing the system.

b. Sophistication of the Analysis System

KoFIU dealt with rising STR filings by advancing the FIU Information System (IT and work process improvements), not by increasing the number of staff.

First, to effectively handle the exploding number of STR filings, the Third Information Project introduced an intelligent analysis system using rules and scoring models. But for securing the accuracy and reliability of these two models, it was crucial to timely adjust weighted values of each element in line with the rapidly changing financial environments, which was difficult to carry out manually due to a shortage of staff. To address this issue, KoFIU adopted an artificial intelligence technique. This technique made it possible to re-adjust weighted values of each element of rules/scoring models by learning, which in turn consistently monitored rules and scoring models.

Second, as financial environments rapidly change and financial transactions become more and more complex, KoFIU built an integrated link analysis system in order to identify and analyze complicated transaction relations and dispersed crime patterns that were hard to detect with conventional analysis methods. The integrated link analysis system not only helped analysts visually figure out complicated transaction relations by displaying the whole capital flows on one screen in diagram form but also provided for comprehensive information such as link information on related accounts and results of rules/scoring models, helping analysts analyze ML activities from various angles. The system also improved the speed and efficiency of analysis, as well as user environments by providing analysts with related information in a comprehensive manner.

In addition, thanks to the integrated link analysis system, KoFIU could select themes of strategic analysis from various angles, systematically store analysis results, and based on the results, categorize types of crimes for systematic accumulation of knowledge.

Finally, collecting necessary information from relevant authorities takes the most time along with analyzing financial transaction data in the assessment and analysis process. In order to shorten this time, KoFIU built a system to exchange information online with relevant authorities, improving the timely use of data.

2.5.4. Improvements

The Fifth FIU Information Project not only helped the successful implementation of new systems but also raised the efficiency of analysis work, but it was necessary to elaborate the STR form in order to standardize financial transaction information which varied from industry to industry. So, KoFIU, in line with the implementation of the Enhanced CDD procedure in the midst of the Fifth project, revised the STR form by reflecting newly-added information. Along with this, KoFIU standardized the account transaction information that was often requested in the STR analysis process, and had reporting entities attach it when reporting STR. All of these data were data based, and systematically arranged and provided through the integrated link analysis system, greatly improving work efficiency. However, the standardization of account transaction information was carried out centering on banks with larger STRs, which resulted in difficulties in grasping financial transaction flows of securities, insurance, etc., a point of improvement.

2.6. The Sixth Project (Prevention): Establishment of an Support System for Inspection and Supervision

2.6.1. Purpose of Establishment

The sixth FIU Information Project aimed (i) to set up infrastructure for guidance and supervision for financial institutions' implementation of AML systems (Enhanced CDD and anti-terrorist financing systems introduced in December 2007, etc.); and (ii) to reinforce security on information retained by KoFIU. The key requirements of the project can be summed up as follows:

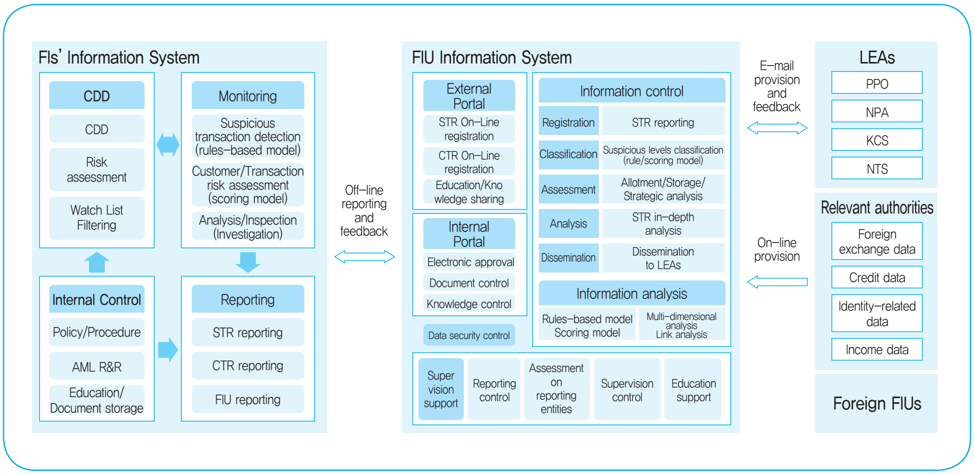
First, it was necessary to build an inspection/supervision support system in order to promptly and effectively assess reporting entities' AML activities. KoFIU's limited workforce was not enough to measure AML implementation states of approximately 6,000 FIs as well as conduct inspection, supervision and graded education.

Second, the FIU Information System stored separately important information such as STR, CTR, administrative data, analysis results and measures taken by LEAs. In order to control these data in a systematic way, KoFIU needed to build an integrated security control system that can protect systems, networks and data from hacking or other illegal hazards, as well as restore them once damage occurs.

2.6.2. Implementation Details

The scope of the sixth FIU Information Project is to establish an inspection/supervision support system and to enhance information security. The composition of the information system established in the sixth project is set out in [Figure 3-19].

Figure 3-19 | Composition of the FIU Information System of the Sixth Project

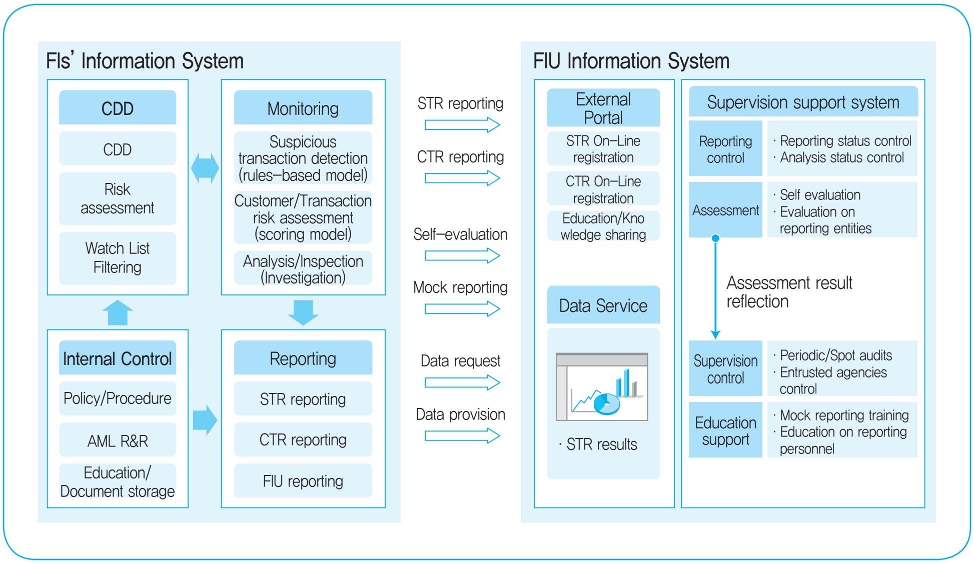


Source: Korea Financial Intelligence Unit

a. Establishment of an Inspection/Supervision Support System

The inspection/supervision support system, as shown in [Figure 3-20] below, consists of reporting/analysis control function, assessment/supervision control function and education support function.

Figure 3-20 | Composition of the Supervision Support System



Source: Korea Financial Intelligence Unit

a) Assessment on Reporting Entities

The reporting entities assessment function is designed to define concrete inspection methods and scoring criteria for each inspection item, providing a base for objective inspection.

b) Assessment and Supervision Control

The assessment and supervision control functions are designed to induce reporting entities to improve their AML activities through their own self-evaluation systems, and for unsatisfactory or risky areas, to intensively control and supervise the areas through the same systems. Also, in line with the Enhanced CDD regime revised in December 2007, KoFIU developed self-evaluation and inspection/supervision checklists.

c) Education Support

The education support function is designed to provide AML-related education to small-sized FIs not accustomed to STR, along with the STR mock training system to support their STR reporting.

b. Enhancement of Information Security

In order to shut off routes that can be exploited by hackers and to effectively control access to important data such as STR and CTR retained by KoFIU, KoFIU reinforced access control on the data server, and expanded electronic equipment to monitor illegal activities and hacking. Also, it built an integrated security control system equipped with functions such as physically separating the database server and the operating program server, monitoring key operation information, storing and analyzing data transfer log data of main server and network, IP control, and remotely backing up data.

2.6.3. Achievements of System Establishment

The major achievement of the Sixth FIU Information Project is to build a support system to objectively assess, control and supervise FIs.

Until then, KoFIU conducted inspections focusing on successful carrying out the AML regime, so actual inspections were conducted by entrusted agencies according to their own plans, with KoFIU assisting for only a small number of inspections. Also, due to a relatively small number of inspectors compared to a large number of reporting entities, the selection of institutions to be inspected and the actual inspections were carried out in a perfunctory manner. In order to tackle this problem, KoFIU adopted a risk-based inspection system.

Also, for the effective implementation of this inspection system, KoFIU developed an assessment index on FIs, by combining general and reporting records, STR analysis results, actions taken by LEAs, etc. Also, it developed a system that can consistently monitor inspections.

The assessment index is divided into three sectors: STR-related sector, new system-related sector (CTR, CDD), and others (internal control, etc.). The index gave high weighed values to the STR-related sector such as growth rate of STR filings, accuracy of report content and dissemination rate to LEAs, putting an emphasis on STR. The index also included general records such as appropriateness of new system implementation, appropriateness of internal report system establishment, whether it prepares enforcement guidelines and AML-related education and training records, while defining each item for objective scoring.

Furthermore, KoFIU set up an inspection control system for controlling inspection plans and results of entrusted agencies, as well as a supervision control system featuring a communications function with entrusted agencies.

2.6.4. Improvements

The Sixth FIU Information Project produced an infrastructure for inspection and supervision in terms of the system, but there was still much to be done in terms of the process. Therefore, it was necessary to establish a mid- and long-term education road map for enhancing inspection, supervision and systematic education on FIs.

a. Improvement of Inspection and Supervision Processes

As shown in <Table 3-12> and [Figure 3-21], the number of FIs inspected by entrusted agencies was approximately 2,500 in 2008, 2,100 in 2009, and 1,700 in 2010, showing a gradual decline since the Sixth FIU Information Project. The average inspection rate also slumped from 28.04% in 2008 to 19.21% in 2010, indicating that inspection/supervision processes had not improved in terms of quantity. Also, the number of inspectors of entrusted agencies, a factor that represents the quality of inspection was not improved. So, in order to carry out more effective inspections, it is crucial to improve the inspection/supervision processes by enhancing inspection authority, inspection supervision, and follow-up management.

Table 3-12 | Inspection Rates of Entrusted Agencies by Year

Classification	2008			2009			2010		
	No. of FIs subject to inspection	No. of inspected FIs	Inspection rate	No. of FIs subject to inspection	No. of inspected FIs	Inspection rate	No. of FIs subject to inspection	No. of inspected FIs	Inspection rate
Korea Post	2,750	398	14.47%	2,750	287	10.44%	2721	148	5.44%
BOK	1,424	292	20.51%	1,424	210	14.75%	1293	256	19.80%
FSS	546	75	13.74%	546	61	11.17%	595	46	7.73%
NACF	1,181	532	45.05%	1,181	594	50.30%	1168	568	48.63%
NFFC	92	48	52.17%	92	46	50.00%	90	43	47.78%
NFCF	133	187	140.60%	133	87	65.41%	133	81	60.90%
NACUFOK	982	251	25.56%	982	250	25.46%	961	194	20.19%
KFCC	1,501	691	46.04%	1,501	443	29.51%	1480	257	17.36%
SMBA, etc.	552	95	17.21%	552	146	26.45%	415	108	26.02%
Total	9,161	2,569	28.04%	9,161	2,124	23.19%	8,856	1,701	19.21%

Source: KoFIU

Figure 3-21 | Change of Inspection Rates by Entrusted Agency

Source: Korea Financial Intelligence Unit

a) Improvement of Inspection Work by Entrusted Agencies

Entrusted agencies have carried out inspections in a cursory and passive way due to the shortage of inspectors and different characteristics of FIs. Also, inspection methods used by each agency lacked coherence and consistency. To resolve this problem and reinforce KoFIU's inspection and supervision functions, KoFIU needs to secure professional inspectors, to adopt a risk-based inspection system for systematic detection of reporting entities with poor AML performances, and to compose inspection manuals.

b) Enhancement of KoFIU's Inspection/Supervision Authorities

In fact, it is almost impossible to review all inspection results conducted on around 2,000 FIs per year and to provide feedback on them. So, the practical way to implement effective inspections is to educate inspectors of entrusted agencies about inspection directions and methods in advance with on-the-job training (OJT) programs. In addition, in order to continue to improve inspection quality, KoFIU needs to set up procedures with which KoFIU can review and analyze inspection results and offer regular feedback to entrusted agencies.

c) Reinforcement of a Follow-up Monitoring System

KoFIU assists entrusted agencies in inspecting about six FIs per year due to the lack of manpower, but even follow-up monitoring for them is not carried out well. To solve this problem, KoFIU needs to build a follow-up inspection system, which regularly checks measures taken by reporting entities after receiving inspection results.

b. Development of Customized Education Content and System

The success of the AML system depends on executives and employees of FIs who are in direct contact with customers. Therefore, it is vital to educate them about recent trends of ML, newly-adopted systems, ML techniques, etc.

KoFIU's education policy is to provide off-the-job training to inspectors and executives, and to induce them to educate their own employees. Large-sized FIs are successfully conducting this job by inviting outside experts or through their own education systems, while small-sized reporting entities that have no education system are finding difficulties in doing this. Advanced countries, including Australia, adopt e-learning system, develop education content by size of FIs, industry, etc., operate about 80 sessions of various kinds, and hold as many as 120 conferences every year. By contrast, KoFIU provides just around 14 off the job trainings a year, and its education content covers the general understanding of the AML system, internal control, STR preparation guidelines, analysis cases, etc. In short, the scope of education is not subdivided, and the contents are not customized. Also, FIs' self education is being carried out in a cursory manner. Therefore, in order to improve the quality of education, it is necessary to regularly check implementation states of education.

Chapter 4

Conclusion

Conclusion

After the *Financial Transaction Reports Act* and the *Proceeds of Crime Act* were passed by the National Assembly in September 2001, KoFIU started the First FIU Information Project in 2002 and completed the Sixth FIU Information Project in 2008, pouring an enormous amount of money into the development of the information system every year. In terms of institution, as described in Chapter 1 through Chapter 3, KoFIU has succeeded in soft-landing the AML/CFT framework according to the 'road map for implementation of FATF Recommendations,' thus obtaining full membership of the FATF and elevating the nation's status in the international community. And in terms of the information system, KoFIU developed the FIU Information System, meeting the requirements of the FIU Information System Maturity Model (FISM), or a model of KoFIU's FIS Information System. When constructing the FIU system, KoFIU built a nation-wide information network, thereby promoting cooperation with relevant authorities and FIs as well as improving analysis efficiency. Also, the superiority of KoFIU's FIS Information System was recognized at home and abroad, raising its reliability.

1. Soft-landing of the AML System through the Action Road Map

As shown in Chapter 1, Korea's AML system was introduced in three stages spanning seven years: STR reporting system in 2001, CTR and CDD regimes in 2005, and the Enhanced CDD procedure and the *Prohibition of Financing for Offences of Public Intimidation Act* in 2007. Also, KoFIU established the AML system in a short time without many hiccups. To achieve this, KoFIU emphasized three main things when implementing the AML system.

First, unlike other countries that adopted the AML system en bloc, KoFIU phased in the system considering local financial environments. In 1993, Korea enforced the real-name financial transaction system (a system that obligates FIs to verify all customers' real names and resident registration numbers), already carrying out part of the CDD obligation required by the FATF. Considering this, KoFIU first implemented STR reporting system, or a key of the AML system, and then phased in CTR, CDD, etc.

Second, KoFIU organized task force teams (TFTs) with relevant authorities and FIs prior to the enforcement of new systems, figured out requirements, and set up implementation plans. For example, in 2008, in preparation for the enforcement of the Enhanced CDD procedure, KoFIU formed TFTs with relevant authorities and FIs, identified possible deficiencies for each FATF Recommendation, and formulated detailed action plans over one year. In addition, KoFIU improved relevant entities' understanding of the AML system through the TFTs, fostering AML experts without a special education curriculum.

Third, in order to minimize the work vacuum until the completion of relevant information systems, KoFIU established the work process and system requirements prior to the enforcement of new systems, and reflected them in the FIU Information System. When establishing the work process, it formed TFTs with reporting entities and offered guidelines on the process, thereby minimizing their confusion. Along with this, KoFIU promoted the necessity of implementing the system in the rapidly changing financial environments through TV and radio ads, posters and meetings, which in turn reduced the general public's resistance to the system.

2. Enhancement of the National Status through the FATF Membership

In order to obtain FATF's full membership, Korea received mutual evaluation from a FATF-APG joint team over two years (From 2008 to 2009), but the result of the initial mutual evaluation report fell far short of the minimum rating the FATF set for full membership. However, thanks to the government's firm determination and close collaboration among relevant authorities, FIs, private enterprises, etc., Korea became the 35th full member of the FATF in October 2009, fulfilling its long-time goal set back when it introduced the AML/CFT framework in 2001 and contributing to raising Korea's status in the international community. Preparing for the FATF membership, KoFIU made extra efforts in the following areas.

First, KoFIU thoroughly reviewed the FATF Recommendations prior to mutual evaluation, and for items not meeting each FATF Recommendation, set up guidelines for their actual implementation, being fully prepared for the evaluation in collaboration with FIs.

Second, despite the low rating of the initial mutual evaluation report, KoFIU provided detailed evidence and countermeasures, such as precedents of the Supreme Court, for each item that was not properly assessed since there was no specific provision in the law during the two rounds of evidence submission periods. And in October 2009, Korea became the 35th full member of the TAFT on the condition that the nation would submit the follow-up report to the FATF.

Third, KoFIU composed the follow-up report in close collaboration with Financial Services Commission, relevant authorities (PPO, NPA, MOJ, entrusted agencies, etc.) and private enterprises (FIs, casinos, etc.), and succeeded in showing the Korean government's strong will to implement the AML system to FATF members.

3. Establishment of the FIU Information System Meeting the FISM Standards

In order to minimize the work vacuum between the passage of AML-related legislation in September 2001 and the establishment of the FIU Information System, KoFIU defined reporting forms necessary for the STR regime and distributed them to FIs in advance. Also, to effectively carry out system development, it set up a short- and long-term master plan for construction of the FIU Information System, considering KoFIU's major businesses, and the information system establishment states of advanced countries.

The master plan divides the construction process into four stages with six projects: introduction stage (1st and 2nd year), development stage (3rd to 4th year), maturity stage (5th to 6th year) and expansion stage (7th year). This construction strategy is in line with that of the FIU Information System Maturity Model (FISMM), developed to assess other countries' FIU information systems in 2009, indicating that the construction of the FIU Information System was carried out in a systematic manner from the beginning. FISMM consists of a total of 15 categories, and recommends the following targets for each stage: establishing an on-line reporting system and an information control system, and automating information collection from relevant authorities in the first introduction stage; building information analysis and inspection supervision systems in the second development stage; and data quality control and advancement of information analysis system in the third maturity stage.

Furthermore, while implementing the projects, KoFIU grasped construction states for each target and analyzed construction cases of advanced countries, and concluded that the construction of the system itself was not enough. Therefore, it formulated the work process and system requirements through consulting, and adopted a phase-in establishment method.

4. Establishment of a Nation-wide AML Information Network

To effectively operate the AML system, it is essential to build close networks among FIs that directly contact customers, KoFIU that analyzes STRs, relevant authorities that provide necessary information and LEAs that are in charge of indictments for ML activities. So, KoFIU considered this from the early stage of setting up the 'FIU Information System master plan', putting an emphasis on building a nation-wide information network. To build the network, KoFIU focused on the following:

First, KoFIU built communications channels with FIs as well as an online STR reporting system in the second and fourth projects. For establishment of the online STR reporting system, KoFIU subdivided the contents of STR into the data of the suspect, transaction data, the data of the other party of transaction, etc. and data based this information. It also applied rules-based and scoring models in order to automatically assess risk levels of STRs using this data even from the STR registration stage.

Second, KoFIU built an intelligent analysis system, thereby raising analysis efficiency. The number of STR filings went up to 24,149 cases in 2006, and soared to 329,463 cases in 2011 (a whopping 24.5-fold hike against 2005), but the number of KoFIU's analysts inched up from 21 persons in 2006 to 26 persons in 2011. Consequently, KoFIU needed to improve the analysis process and system to identify and analyze STRs with higher suspicious levels with a limited workforce. To this end, KoFIU improved the allotment process by adopting rules and scoring models, and built an integrated link analysis system, which displays relevant data on one screen and financial transactions in time order in in-depth analysis, along with the Knowledge Management System (KMS) where analysts can share their analysis knowledge and know-how. With the introduction of these systems, the ratio of in-depth analysis to STR filings fell from 43.44% in 2005 to 5.01% in 2011 (a staggering 38.43% decline), but the dissemination rate to LEAs surged from 30.77% in 2005 to 79.48% in 2011 (a whopping 48.71% hike), representing increased analysis efficiency. In addition to this, the STR registration, analysis and dissemination period was reduced from 55 days in 2004 to 45 days in 2005, and 32 days in 2008, an evidence of increased productivity per analyst.

Third, KoFIU set up a database for information from relevant authorities, including MOPAS (family register data), NTS (tax data), the Supreme Court (family register data), KCS (clearance data), MOJ (immigration data) and others (health and unemployment insurance data, etc.), thus shortening the information collection period and achieving a more timely use of data. Unlike the U.S. or Japan that built a partial database, Korea set up a comprehensive administrative information network at the national level, starting from the Informatization of Public Administration project in 1978 to the e-government road map in the 2000s. As a result, Korea's e-government project won first place in the UN's e-government development index and online e-participation index for two consecutive years in 2010 and 2011.

Finally, in order to maintain cooperative relationships with LEAs, KoFIU set up and is operating human resources and information exchange systems. For personal exchange, staff of each LEA is dispatched to KoFIU to conduct analysis work in their area of expertise as well as to play a role as a mediator between KoFIU and their agency. As for information exchange, LEAs appoint a person in charge of STR and give KoFIU feedback on their investigation states on disseminated STRs and investigation results.

After KoFIU's efforts to establish an information network for national AML, it could cooperate with foreign FIUs and detect an organized international financial crime in 2012. The organized international financial crime, whose ringleader was Nigerian, hacked customers' information from 39 banks in the United States, obtained mortgage loans and used at least six countries (South Korea, Japan, Malaysia, Indonesia, Singapore and Thailand) as platforms for money laundering. In this case, KoFIU detected 68 cases of money laundering (more than $10,000) in Korea. In addition, it could prevent additional damage by cooperating with Japan and other countries.

Also, by using an intelligent analysis system that can conduct effective analysis on reported STR through communication channels with financial institutions as well as cooperation with LEAs, KoFIU tracked down complicated and various cases of money laundering which are increasingly more sophisticated , including the embezzlement of tens of billions of project settlement dollars, unlicensed sale of pseudo-petroleum, evasion of taxes on foreign income, evasion through a false name bank account, multi-level bank fraud, voice phishing fraud and illegal foreign exchange transactions by means of diversified remittance.

5. FIU Information System Recognized at Home and Abroad

KoFIU's FIU Information System contributed to the innovation of AML activities by applying top-notch technologies such as artificial intelligence to assessment and analysis work. In recognition of that contribution, the FIU Information System won the Intelligent

Business Grand Prize awarded by Korea Intelligent Information System Society in 2006, and took 2nd place in Korea's e-business Grand Prize in 2007 jointly sponsored by the Ministry of Commerce, Industry and Energy and the Korea Institute for Electronic Commerce. These accolades represent Korea's superior FIU Information System and KoFIU's systematic innovation that were recognized by outside authorities.

Also, the Asia-Pacific Group on Money Laundering (APG) chose Korea as a development model of the AML system for late starters in the Asia-Pacific region, and asked Korea for technical assistance, which indicates that Korea's excellent AML system and FIU Information System was globally recognized. To meet the demands of the international community, KoFIU has provided technical support, including policy consulting for improvement of the AML system, establishing strategies for FIU information system development and operation, IT assistance, education and training by invited outside experts, to 10 countries such as Mongolia, Vietnam and Nepal since 2011, based on its experiences and know-how in the development, establishment and operation of the AML/CFT framework and the FIU Information System.

An, Hyeong-do and Kim, Jong-Hyeok (2005), "Anti-money Laundering Obligation of Non-financial Businesses and Professions: Management Cases and System Introduction of Major Countries," *Korea Institute for International Economic Policy*

Financial Intelligence Unit (2007), "Modernization of the Anti-money Laundering System," *Financial Intelligence Unit of the Ministry of Finance and Economy*

Jang, Il-seok (2005), "Understanding of the Anti-money Laundering System," *Woori Planning*

Kim, Jae-sik and Jeong, Hui-cheol (2007), "Understanding and Countermeasures of the Anti-money Laundering System," *Samil PricewaterhouseCoopers*

Ahn, Jong-Byum (1993), "the real-name financial transaction system and the nation's economy," *Korea Institute of Public Finance*

Korea Financial Intelligence Unit (2005), "2004 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2006), "2005 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2007), "2006 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2008), "2007 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2009), "2008 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2010), "2009 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2011), "2010 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

Korea Financial Intelligence Unit (2012), "2011 Annual Report," *Korea Financial Intelligence Unit of Financial Services Commission*

www.ksp.go.kr

Ministry of Strategy and Finance, Republic of Korea

339-012, Sejong Government Complex, 477, Galmae-ro, Sejong Special Self-Governing City, Korea Tel. 82-44-215-2114 www.mosf.go.kr

KDI School of Public Policy and Management

130-722, 85 Hoegiro Dongdaemun Gu, Seoul, Korea Tel. 82-2-3299-1114 www.kdischool.ac.kr

ISBN 979-11-5545-046-8

Knowledge Sharing Program
Development Research and Learning Network

- 130-722, 85 Hoegiro Dongdaemun Gu, Seoul, Korea
- Tel. 82-2-3299-1071
- www.kdischool.ac.kr