CHAPTER III

THE ELEMENTS OF AN EFFECTIVE AML-CFT FRAMEWORK

1 Legal system requirements

The degree of emphasis on certain areas of legal system of jurisdictions may vary although the legal system requirements for AML-CFT for a country should be based upon the FATF 40 + 9 Recommendations that are mandates for all countries, and countries should consult the FATF methodology for AML-CFT (June 2006) for further explanations of these requirements. Different countries have different history of vigorous action against criminal activities involving the monetary system. Depending on the problems they have faced, policy makers of countries should heavily focus on their systems and measures. For example, in the countries like Saudi Arabia affected by terrorist attacks, authorities put more emphasis on the measures to counter terrorism and the financing of terrorism whereas in the countries like Thailand with drug-trafficking and human-trafficking problems, authorities are more attentive to the measures against money laundering related to drug-trafficking and human-trafficking. As Singapore, the fifth-biggest currency trading center in the world and the second biggest in Asia after Tokyo, has figured on a US State Department list since 2004 as a center of "primary concern" for money laundering[1] it emphasizes introducing more new measures to try to detect money laundering and terrorism financing effectively. Lessons through experiences and recommendations produced by the evaluation teams from standard setters help policy makers improve and upgrade the standards of their respective AML-CFT systems to be more effective and efficient.

1.1 AML-CFT system

In order to establish a strong and effective AML-CFT system with comprehensive rules covering anti-money-laundering and counter-terrorist financing requirements for both banking and non-banking sectors, it is essential to set up an adequately operational legal and institutional or administrative framework not only with the regulatory power that provides competent authorities with the necessary duties, powers and sanctions but also with the laws that create money laundering and terrorist financing offenses, plus enforcement power that provides for freezing, seizing and confiscation of the proceeds of crime and terrorist funding. The effective AML-CFT system also includes laws and regulations that impose the required obligations on financial institutions and designated non-financial businesses and professions, and other enforceable means that give a country the ability to provide the widest range of international cooperation.

The criminalization of money laundering and financing of terrorism, in accordance with Article 3(1) (b) and (c) of the Vienna Convention (1988) and Article 6 (1) of the Palermo Convention (2000), and the criminalization of terrorist financing in line with

---

[1] "New rules aim to detect money laundering"- News report on business section, The Bangkok Post, 29 October 2007

Article 2, read in conjunction with Article 7 of the Convention against Financing of Terrorism (1999), focus on 3 important factors: (1) compliance with AML-CFT preventive measures, (2) acting against offenders and (3) international cooperation in this critical law enforcement function.

Since the UNSC Resolution 1617 (2005), paragraph 7 strongly urges all member States to implement the FATF Forty Recommendations on money laundering and Nine Special Recommendations on terrorist financing, they are mandates for action by every country. Although there are 20 designated categories of offenses according to the FATF Glossary of the Forty Recommendations, countries are encouraged to go beyond this[2]. The essential requirement is to criminalize the proceeds derived from any type of conduct related to the 20 designated categories. A country must include "a range of offenses" within each of the designated categories of offenses in accordance with its domestic laws, and the specific legal method of criminalization is left to the discretion of the country concerned.

According to the findings from the AML-CFT assessments[3] by the IMF and the WB, overall level of compliance in all assessed countries is low.

> *21 percent of all recommendations were rated fully compliant, 24 percent were rated largely compliant, 29 percent were rated partially compliant, and 26 percent non-compliant.*

The findings also show that compliance for the FATF Forty Recommendations (47 % fully or largely compliant) is better than that for the Nine Special Recommendations (33% fully or largely compliant).

Regarding legal system, although all assessed countries have criminalized ML, the list of ML offenses in 42% of the assessed countries does not fully comply with the FATF standard as it does not cover all the relevant circumstances reflected in the standard. Besides, 44% of assessed countries were rated non-compliant on criminalizing the FT.

A vital attribute of any legal frame is to have laws and regulations working together without contradiction. In order to effectuate AML-CFT requirements, it must be ensured that the financial secrecy laws do not inhibit implementation of the FATF Recommendations[4].

Most of the assessed countries' bank secrecy laws were positively assessed as not inhibiting the implementation of the FATF Recommendations in AML-CFT assessments[5].

---

2 Recommendation 1, Essential Criteria 1.3

3 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

4 FATF Recommendation 4

5 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

1.2 Competent authorities

Although the legal and institutional or administrative framework with regulatory power provides the competent authorities with necessary powers, if they cannot avoid corruption, that particular AML-CFT regime will become an ineffective regime. The competent authorities, therefore, take an important role in fighting money laundering and terrorist financing. The 2004 FATF Forty Recommendation 30 states:

> *Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.*

As mentioned above, since competent authorities are crucial for combating money laundering and terrorist financing, significant cooperation between competent authorities is an effective factor to support their performance. Regarding cooperation and coordination among competent authorities, the 2004 FATF Recommendation 31 says:

> *Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to cooperate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.*

1.3 Investigation and confiscation

The AML-CFT laws and mechanisms should facilitate cooperation and coordination among competent authorities who are responsible for money laundering and terrorist financing investigations so as to obtain effective international cooperation including mutual legal assistance. Special investigative techniques and mechanisms should be developed and authorities concerned should exert every effort in cooperative investigations with other countries as well. According to the AML-CFT assessments[6], none of the assessed countries were considered fully compliant with the FATF standard although it was generally rated favorably.

It is needless to say that fighting against international crime and terrorist financing will not lead to the achievement without effective confiscation laws. The Vienna and the Palermo Conventions define the term "proceeds of crime" and prescribe laws that permit the confiscation of the proceeds of laundering and predicate offenses without mentioning "terrorist financing". The revised FATF Special Recommendation II, however, encourages countries to ensure that the financing of terrorism and associated money laundering predicate offenses are designated as money laundering predicate offenses. The FATF also encourages countries to adopt confiscation laws relating to property laundered and proceeds from money laundering or predicate offenses[7] and terrorist assets[8] in accordance with the Vienna and the Palermo Conventions, and the

---

6 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

7 FATF Recommendation 3

8 FATF Special Recommendation III

UN Resolutions relating to the prevention and suppression of the financing of terrorist acts.

For the enforcement of confiscated property, the Vienna Convention –Article 5 (3) states:

> *In order to carry out the measures referred to in this article, each Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A Party shall not decline to act under the provisions of the paragraph on the ground of bank secrecy.*

The international law on confiscation does not preclude the rights of *bona fide* third parties (the third parties in good faith). The Vienna Convention [Article 5 (8)] and the Palermo Convention [Article 12 (8)] clearly state:

> *The provision of this Article shall not be construed as prejudicing the rights of bona fide third parties.*

There are 2 necessary steps[9] to eliminate the profitability of international money laundering activities:

1. Establishing an effective confiscation regime for domestic purposes
2. Creating cooperative mechanisms for enforcing cross-border confiscation order

The Vienna Convention [Article 5-5(a) and 5(b)] and the Palermo Convention [Article 14-1, 14-3(a) and 3(b)] state that confiscated proceeds or property shall be disposed of by that party according to its domestic law and administrative procedures.

Regarding freezing and confiscation, according to the findings from the AML-CFT assessments[10] by the IMF and the WB, the report states:

> *Compliance regarding SR III on freezing and confiscation of terrorist assets is weak. No countries were fully compliant, 11 percent largely compliant, 50 percent partially compliant and 39 percent non-compliant. Despite identified flaws in the legal framework, the assessed countries have adopted transitional measures to implement UN Security Council Resolution 1267 and successor resolutions on terrorist financing.*

1.4 Financial institutions

According to the FATF, financial institutions are defined as "any person or entity who conducts as a business one or more of the following activities or operations on behalf of a customer."

---

9 WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p.V-9

10 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

1. *Acceptance of deposits and other repayable funds from the public*[11].
2. *Lending*[12].
3. *Financial leasing*[13].
4. *The transfer of money or value*[14].
5. *Issuing and managing means of payment (e.g. credit and debit cards, checks, traveler's checks, money orders and banker's drafts, electronic money).*
6. *Financial guarantees and commitments.*
7. *Trading in:*
   (a) Money market instruments (checks, bills, CDs derivatives, etc);
   (b) Foreign exchange;
   (c) Exchange, interest rate and index instruments;
   (d) Transferable securities; and
   (e) Commodity futures trading.
8. *Participation in securities issues and the provision of financial services related to such issues.*
9. *Individual and collective portfolio management.*
10. *Safekeeping and administration of cash or liquid securities on behalf of other persons.*
11. *Otherwise investing, administering or managing funds or money on behalf of other persons.*
12. *Underwriting and placement of life insurance and other investment related insurance*[15].
13. *Money and currency changing.*

1.5 Non-financial institutions

There are 2 types of non-financial institutions apart from the aforementioned financial institutions. They are designated non-financial businesses and professions (DNFBPs) and non-designated non-financial businesses and professions (NDNFBPs).

1.5.1 Designated non-financial businesses and professions

The 2004 revised FATF Recommendations include certain designated non-financial businesses and professions (DNFBPs) within coverage of the Forty Recommendations[16] as follows:

a) Casinos (which also includes internet casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these

---

11 This also captures private banking .
12 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).
13 This does not extend to financial leasing arrangements in relation to consumer products.
14 This applies to formal and informal sectors, such as, alternative remittance activity.
15 This applies to both insurance undertakings and intermediaries, such as agents and brokers.
16 Data attachment 1 (A)

Recommendations, and which as a business, provide any of the following services to third parties:

- *acting as a formation agent of legal persons;*
- *acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;*
- *providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;*
- *acting as (or arranging for another person to act as) a trustee of an express trust;*
- *acting as (or arranging for another person to act as) a nominee shareholder for another person.*

These institutions are categorized into two[17]: (1) casinos, and (2) all other non-financial businesses and professions. The following points are strictly required for the casinos.

- Licensing;
- Measures to prevent casinos being owned, controlled or operated by criminals; and
- Supervision of their compliance with AML-CFT requirements.

For all other non-financial businesses and professions such as lawyers, notaries, auditors and accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones, effective systems for monitoring – carried out either by a government agency or a self-regulatory organization – and ensuring compliance on a risk-sensitive basis are to be put in place.

Regardless of the types of financial institutions, countries have to make sure that financial institutions are not controlled by the criminals. The financial institutions, consequently, are subject to comprehensive supervisory regimes as set out in the standards issued by the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors, and the International Organization of Securities Commissioners. The requirements applicable to DNFBPs are more limited and they are not normally subject to the same stringent requirements as Core Principles Institutions for the same prudential issues do not arise.

1.5.2 Non-designated non-financial businesses and professions

FATF Recommendation 20 states that the FATF 40+9 Recommendations should be applied to businesses and professions, other than designated non-financial businesses and professions that pose a money laundering or terrorist financing risk. Businesses relating to high value and luxury goods and pawnshops are some examples of non-designated non-financial businesses and professions (NDNFBPs).

---

[17] WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: pp.V-25 – V-26

2 Preventive measures

In order to prevent financial institutions from being used by criminals, internal policies which vary depending on the type and size of a particular financial institution and the scope and nature of its operation need to be in place. Internal policies should include ongoing training that keeps employees well-informed of the latest developments on AML and CFT. One important point, among others, is that adequate screening procedures should be done when hiring employees. Recommendation 15 states:

> *Financial institutions should develop programs against money laundering and terrorist financing. These programs should include:*
>
> *a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.*
> *b) An ongoing employee training program.*
> *c) An audit function to test the system.*

Above all, as long as criminals control financial institutions or hold senior management positions in financial institutions, it is extremely difficult for countries not only to prevent but also to detect the crimes, and consequently they tend to pose dangerous obstacles to combating money laundering and financing of terrorism. Integrity standards can help prevent criminals from participating in AML-CFT activities. Countries should not only impose AML-CFT preventative measures in legislation but also make sure that the requirements are implemented in practice. Recommendation 23, paragraph 1, reads:

> *Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.*

Measures to prevent the unlawful use of legal entities by money launderers and terrorist financiers are crucial to be taken. Moreover, appropriate measures to ensure that bearer shares of securities, trust and similar legal arrangements are not misused by the criminals involved in the twin evils, money laundering and financing of terrorism. Recommendation 33 states:

> *Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.*

More emphasis should be placed on preventive measures than seizure, confiscation

and forfeiture of assets. Authorities should prevent the occurrence of money laundering and financing of terrorism in the first instance rather than let the criminals carry out illicit performance to obtain dirty profits at the highest magnitude and confiscate the proceeds. FATF Recommendations 5 – 25 are for preventive measures.

2.1 Know your customer/Customer due diligence (KYC/CDD)

The importance of Know Your Customer/Customer Due Diligence (KYC/CDD) has been recognized by supervisors of financial institutions in the world community and they have been working hard to have adequate policies and procedures in place, including "Know Your Customer" / "Customer Due Diligence", which will ensure compliance with the money laundering legislation in force and promote high ethical standards in the financial sector and prevent the financial institutions being used intentionally or unintentionally by criminals.

It is essential to find out if the customer is acting on his/her own or on behalf of another person. Core Principle 18 deals with an important part of AML-CFT institutional framework "Know Your Customers". The following are 12 essential criteria and 1 additional criterion for Core Principle 18[18].

Essential criteria

1. *Laws or regulations clarify the duties, responsibilities and powers of the banking supervisor and other competent authorities, if any, related to the supervision of banks' internal controls and enforcement of the relevant laws and regulations regarding criminal activities.*

2. *The supervisor must be satisfied that banks have in place adequate policies and processes that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, for criminal activities. This includes the prevention and detection of criminal activity, and reporting of such suspected activities to the appropriate authorities.*

3. *In addition to reporting to the financial intelligence unit or other designated authorities, banks report to the banking supervisor suspicious activities and incidents of fraud when they are material to the safety, soundness or reputation of the bank.*

4. *The supervisor is satisfied that banks establish "know-your-customer" (KYC) policies and processes which are well documented and communicated to all relevant staff. Such policies and processes must also be integrated into the bank's overall risk management. The KYC management program, on a group-wide basis has as its essential elements:*
   - *a customer acceptance policy that identifies business relationships that the bank will not accept;*
   - *a customer identification, verification and due diligence program; this encompasses verification of beneficial ownership and includes risk-based reviews to ensure that records are updated and relevant;*
   - *policies and processes to monitor and recognize unusual or*

[18] Basel Committee on Banking Supervision, Core Principles Methodology, October 2006: pp. 25 – 26

potentially suspicious transactions, particularly of high-risk accounts;

- *escalation to the senior management level of decisions on entering into business relationships with high-risk accounts, such as those for politically exposed persons, or maintaining such relationships when an existing relationship becomes high-risk; and*
- *clear rules on what records must be kept on consumer identification and individual transactions and their retention period. Such records should have at least a five-year retention period.*

5. *The supervisor is satisfied that banks have enhanced due diligence policies and processes regarding correspondent banking. Such policies and processes encompass:*

   - *gathering sufficient information about their respondent banks to understand fully the nature of their business and customer base, and how they are supervised; and*
   - *not establishing or continuing correspondent relationships with foreign banks that do not have adequate controls against criminal activities or that are not effectively supervised by the relevant authorities, or with those banks that are considered to shell banks.*

6. *The supervisor periodically confirms that banks have sufficient controls and systems in place for preventing, identifying and reporting potential abuses of financial services, including money laundering.*

7. *The supervisor has adequate enforcement powers (regulatory and /or criminal prosecution) to take action against a bank that does not comply with its obligations related to criminal activities.*

8. *The supervisor must be satisfied that banks have:*

   - *requirements for internal audit and/or external experts to independently evaluate the relevant risk management policies, processes and controls. The supervisor must have access to their reports;*
   - *established policies and processes to designate compliance officers at the management level, and appointed a relevant dedicated officer to whom potential abuses of the bank's financial services (including suspicious transactions) shall be reported;*
   - *adequate screening policies and processes to ensure high ethical and professional standards when hiring staff; and*
   - *ongoing training programs for their staff on KYC and methods to detect criminal and suspicious activities.*

9. *The supervisor determines that banks have clear policies and processes for staff to report any problems related to the abuse of the banks' financial services to either local management or the relevant dedicated officer or to both. The supervisor also confirms that banks have adequate management information systems to provide managers and the dedicated officers with timely information on such activities.*

10. *Laws and regulations ensure that a member of a bank's staff who reports suspicious activity in good faith either internally or directly to the relevant authority cannot be held liable.*

> *11. The supervisor is able to inform the financial intelligence unit and, if applicable, other designated authority of any suspicious transactions. In addition, it is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.*
>
> *12. The supervisor is able, directly or indirectly, to cooperate with the relevant domestic and foreign financial sector supervisory authorities or share with them information related to suspected or actual criminal activities where this information is for supervisory purposes.*
>
> ***Additional criteria***
>
> *1. If not done by another authority, the supervisor has in-house resources with specialist expertise for addressing criminal activities.*

The FATF's KYC/CDD based on the Basel Committee's KYC/CDD is more closely associated with combating ML and FT, not like the Basel Committee's approach to KYC/CDD where sound KYC/CDD procedures are seen as a critical element in the effective management of banking risks and they are critical in protecting the safety and soundness of banks and the integrity of banking systems. Nonetheless, the Committee supports the adoption and implementation of the FATF Recommendations. One of the purposes to review the Core Principles is to enhance consistency between the Core Principles and the corresponding standards for securities and insurance as well as for anti-money laundering and transparency, and the Basel Committee and the FATF have been working together and will continue to maintain close contact with each other.

Customer Due Diligence – adequate due diligence on new or existing customers – is a key part of AML-CFT policy without which banks can become subject to reputational, operational, legal and concentration risks in banking systems. It is also stated in Provision 30 of the Basel Committee "Customer Due Diligence for Banks" that a numbered account – the name of the beneficial owner known to the financial institution only that is substituted by an account number – should be subject to exactly the same KYC/CDD procedures as all other customer accounts. It reads:

> *Banks should never agree to open an account or conduct ongoing business with a customer who insists anonymity or who gives a fictitious name. Nor should confidential numbered[19] account function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by the selected staff. Whereas a numbered account can offer additional protection for the identity of the account holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.*

FATF Recommendation 5 also states that financial institutions should not keep anonymous accounts or accounts in fictitious names and when they should undertake

---

[19] In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

CDD measures.

> *Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.*
>
> *Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:*
>
> - *establishing business relations;*
> - *carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;*
> - *there is a suspicion of money laundering or terrorist financing; or*
> - *the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.*
>
> *The customer due diligence (CDD) measures to be taken are as follows:*
>
> *a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.*
> *b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.*
> *c) Obtaining information on the purpose and intended nature of the business relationship.*
> *d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.*

2.2 Record-keeping requirements

The CDD and record-keeping requirements for financial institutions, non-financial institutions and designated non-financial businesses and professions are set out in FATF Recommendations 5 to 12. Institutions are required to keep customer identity and transaction records for at least 5 years following the termination of an account[20].

When a new customer is non-resident, special attention should be exercised[21]. Provision 23 of the Basel Committee CDD for banks reads:

> *Banks should 'document and enforce policies of identification for customers and those acting on their behalf[22]'. The best documents for verifying are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has*

---

20 FATF Recommendation 10

21 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, Provision 23

22 Basel Committee on Banking Supervision, Core Principles Methodology, essential criteria 2

chosen to open an account in a foreign jurisdiction.

Having ensured that the financial secrecy laws do not inhibit implementation of the FATF Recommendations, financial institutions must collect the information of the customers as much as they can. Neither an account should be opened without verifying the new customer's identity satisfactorily[23] nor should a customer be permitted to open or maintain an account using an anonymous or fictitious name[24]. The Basel Committee CDD for banks, Provision 22, reads:

> *Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until a new customer is satisfactorily verified.*

The financial institution needs to take measures to verify the identity of the beneficial owner when an agent represents a beneficiary via corporations or other intermediaries. In order to verify the legality of the entity the financial institution should collect the following information from the potential customer[25].

1. Name and legal form of customer's organizations;
2. Address;
3. Names of the directors;
4. Principal owners or beneficiaries;
5. Provisions regulating the power to bind the organization;
6. Agent(s) acting on behalf of the organization; and
7. Account number (if applicable).

The Committee developed a series of recommendations that provide a basic framework for supervisors around the world to be used as guidelines in the development of KYC/CDD practices in their supervised financial institutions. A financial institution should develop and enforce a clear customer acceptance policy and tiered customer identification program that involves more extensive due diligence for high risk accounts and includes proactive account monitoring for suspicious activities[26]. In accordance with international standards set by the Basel Committee on Banking Supervision and by the FATF, countries must ensure that their financial institutions have appropriate customer identification and due diligence procedures in place.

It seems that countries should extremely work hard in order to comply with Recommendation 5 due to the report on the AML-CFT assessments[27] by the IMF and the WB. It states:

> *For customer due diligence (CDD) (Recommendation 5), no countries were rated compliant, 33 percent were considered largely compliant, 67 percent were partially compliant or non-compliant.*

---

23 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, Provision 22

24 ibid.: Provision 30, and FATF Recommendation 5

25 WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p. VI-6

26 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, Provision 20

27 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

2.3 High risk accounts and transactions

Enhanced due diligence measures should be taken into account on the following high risk accounts and transactions[28].

- Politically exposed persons (PEPs)
- Transactions from the countries on the NCCT list
- Shell banks
- Non-face-to-face customers
- Correspondent banking
- Customers introduced by intermediaries
- Insurance sector measures
- Securities sector measures
- Designated non-financial businesses and professions
- Suspicious transactions

2.3.1 Politically exposed persons

Politically exposed persons (PEPs) abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. in countries where corruption is widespread. The definition of PEPs stated in the Glossary of 2004 FATF Forty Recommendations is:

> *PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.*

Although the definition does not apply to the domestic PEPs the 2004 FATF Assessment Methodology relating to Recommendation 6, additional element 6.5, encourages the countries to extend extra due diligence to domestic PEPs. Recommendation 6 encourages the financial institutions to perform the additional measures consisting of the following:

> *Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:*
>
> *a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.*
> *b) Obtain senior management approval for establishing business relationships with such customers.*
> *c) Take reasonable measures to establish the source of wealth and source of funds.*
> *d) Conduct enhanced ongoing monitoring of the business relationship.*

Provisions 41 to 44 in the Basel Committee Customer Due Diligence for Banks

---

[28] WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: pp. VI-8 – VI-13

discuss the matters related to the funds from corrupt PEPs and how to tackle them effectively. Among them, Provision 44 states:

> *Banks should gather sufficient information from a new customer and check publicly available information in order to establish whether or not a customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.*

The report on the AML-CFT assessments[29] by the IMF and the WB states:

> *All assessed high- and middle-income countries have adopted a range of preventive measures applicable to the prudentially-regulated financial sectors (the banking, securities, and insurance sectors), but implementation is uneven. No countries were fully compliant, and a large percentage of the countries were non-compliant with the Recommendation requiring enhanced due diligence for politically exposed persons. Many of the assessed low-income countries had only begun the process of creating regulatory frameworks. Where such frameworks were present, they only covered the banking sector.*

2.3.2 Countries on the NCCT list and shell banks

The PEPs within the NCCTs might create vulnerabilities of the banking system to money laundering since they abuse the power to use the banking system of their own country. Besides the PEPs, criminals might use the banks in the countries on the NCCT list that have weak AML-CFT regimes. It is, therefore, important to carry out adequate due diligence on the transactions from the countries on the NCCT list.

The main objective of the NCCT initiative is to reduce the vulnerabilities of the financial system to money laundering. Countries on the NCCT list are the countries that have failed to make adequate progress in addressing the serious deficiencies previously identified by the FATF. In other words, implementation of measures for the prevention, detection and punishment of ML and FT is not sufficient in accordance with international standards. It is required to identify clients or beneficial owners from these countries before business relationships are established and to enhance surveillance and report financial transactions and other relevant actions involving the countries on the NCCT list.

In addition, if a bank is incorporated in a country but it has no physical presence in that country and is not affiliated with a regulated financial group, transactions from those banks (shell banks) should not be undertaken.

2.3.3 Non-face-to-face customers and correspondent banking

Some of the customers do not present themselves at the financial institutions for their interview when conducting transactions. Financial institutions should, therefore, be aware of non-face-to-face customers and should take necessary steps to deal with them[30]. The topics related to non-face-to-face customers[31] and correspondent

---

[29] IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

[30] FATF Recommendation 8

banking[32] are discussed in detail in the Basel Committee Customer Due Diligence for Banks, (October 2001).

Recommendation 7 states that financial institutions should not only gather sufficient information about the respondent institutions but also assess the respondent institution's AML-CFT controls. In addition, financial institutions should obtain approval from their senior management before establishing new correspondent relationships and document the respective responsibilities of each institution. It reads:

> *Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:*
>
> *a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.*
> *b) Assess the respondent institution's anti-money laundering and terrorist financing control.*
> *c) Obtain approval from senior management before establishing new correspondent relationships.*
> *d) Document the respective responsibilities of each institution.*
> *e) With respect to 'payable-through accounts', be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.*

Non-face-to-face customers usually use postal services and telecommunications networks to obtain financial services for their convenience. However, electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. Although developing technologies provide the customers with luxurious convenience the nature of electronic banking creates difficulties in customer identification and verification[33]. Recommendation 8 states:

> *Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.*

Provision 48 of the Basel Committee CDD for Banks states:

> *In accepting business from non-face-to-face customers:*
>
> - *banks should apply equally effective customer identification procedures for non-face-to-face customers as for those available*

---

31 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, Provisions (45 to 48) and FATF Recommendation 8

32 ibid.: Provisions (49 to 52), and FATF Recommendation 7

33 ibid.: Provision (46)

for interview; and

- *there must be specific and adequate measures to mitigate the higher risk.*

Examples of measures to mitigate the higher risk include:

- *certification of documents presented;*
- *requisition of additional documents to complement those which are required for face-to-face customers;*
- *independent contact with the customer by the bank;*
- *third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36;or*
- *requiring the first payment to be carried out through an account in customer's name with another bank subject to similar customer due diligence standards.*

2.3.4 Intermediaries

When the client account is opened by a professional intermediary that client must be identified[34]. Although the funds held by a professional intermediary or lawyer on behalf of entities are not co-mingled, if there are sub-accounts that can be attributable to each beneficial owner, all beneficial owners of the sub-accounts by the intermediary or lawyer must be identified[35]. When the funds are co-mingled the financial institution should look through to the beneficial owners unless the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries[36]. Regarding customers who are introduced to financial institutions via domestic or international intermediaries, three things should be done[37].

1. Ensure that the intermediary is subject to CDD requirements that its compliance with such due diligence requirements is subject to supervision.
2. Ensure that the intermediary has collected sufficient information about identity and other relevant due diligence documentation about the customer.
3. Ensure that the intermediary can make that information available on request without delay.

2.3.5 Securities firms and insurance companies

The securities firms and the insurance industry can follow and adhere to the relevant requirements stated in the FATF Methodology and CDD requirements and guidelines established and provided by the IOSCO and the IAIS respectively. An Insurance entity must obtain the following information[38].

- Location completed;
- Client's financial assessment;

---

34 Basel Committee, Customer Due Diligence for Banks, Provision 37, and FATF Recommendation 9

35 ibid.: Provision (38)

36 ibid.: Provision 39

37 WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p. VI-11

38 IAIS, Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities, January 2002. http://www.sigortacilik.gov.tr/02YD/24USDBD/USDBD_Dosyalar/Rehber-4.pdf

- Client's need analysis;
- Payment method details;
- Benefit description;
- Copy of documentation used to verify customer identity;
- Post-sale records associated with the contract through its maturity; and
- Details of maturity processing and claim settlement.

When the transaction seems to be unusual and/or when the source of funds cannot be inquired, the financial institutions including insurance sector and securities sector should submit a suspicious transaction report to the authorities for further investigation in accordance with the 2004 FATF Recommendation 13. Insurance companies and securities firms should report suspicious activities to the respective financial intelligence unit or other national centralized authority. The institution is not supposed to investigate the transaction or to obtain the evidence of connection between the funds and any criminal activity, including fiscal crimes.

2.3.6 Designated non-financial businesses and professions (DNFBPs)

The Glossary of the FATF 40 Recommendations defines designated non-financial businesses and professions. (Please see the heading 1.5.1 Designated non-financial businesses and professions.)

Not only the scope and organization of DNFBPs greatly differ from those of the supervised financial institutions but also the scope and responsibilities of lawyers, notaries, auditors and accountants, and the extent of their regulation, vary considerably from country to country. In some countries, entry into the professions is strict and subject to demanding qualifications whereas in others, it is more flexible to come into a profession subject to light regulation. At the same time, they are not familiar with AML-CFT obligations.

Generally real estate agents and dealers in precious metals and stones that offer a range of financial services are very lightly regulated as they are informally organized. Since the AML-CFT obligations have been recently extended to DNFBPs, jurisdictions have to introduce the necessary legal and regulatory framework for their AML-CFT regimes. Likewise, some countries provide a range of financial services (foreign exchange, credit, and payments transfer) in casino operation and some do not even permit casinos at all. In fact, the legal casinos are regulated and have started to apply AML-CFT requirements.

Regardless of their countries, all DNFBPs must follow CDD procedures that apply to casinos, real estate agents, dealers in precious metals and stones, professionals, and trust and company service providers. Recommendation 12 states:

> *The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:*
>
> *a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.*
> *b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.*
> *c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or*

> *above the applicable designated threshold.*
> *d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:*
> - *buying and selling of real estate;*
> - *managing of client money, securities or other assets;*
> - *management of bank, savings or securities account;*
> - *organization of contributions for the creation, operation or management of companies; and*
> - *creation, operation or management of legal persons or arrangements, and buying and selling of business entities.*
>
> *e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.*

According to the report on the AML-CFT assessments[39] by the IMF and the WB, for Recommendation 12, on extending customer due diligence procedures to DNFBPs, no country was rated either fully or largely compliant; 56 percent achieved a partially compliant rating, and 44 percent were non-compliant. It also states:

> *No countries were fully compliant and a large percentage of assessed countries were non-compliant with the Recommendations concerning DNFBPs. Even where AML-CFT requirements had been fully extended to DNFBPs, implementations was weak.*
>
> *Breaking down the findings by income groups, the assessed low-income countries were universally non-compliant on Recommendations 12 and 16 (CDD and STR respectively) and 83 percent non-compliant on Recommendation 24 (supervision). The assessed middle-income countries were 80 percent partially compliant and 20 percent non-compliant on R 12 and 16, and 20 percent largely, 20 percent partially, and 60 percent non-compliant on R 24. The assessed high-income countries received ratings on R 12 similar to those of the middle-income countries (71 percent partially and 29 percent non-compliant), did somewhat better on R 16 (14 percent largely, 57 percent partially, and 29 percent non-compliant), and on R 24 (14 percent largely, 43 percent partially and 43 percent non-compliant).*

Regulatory and supervisory measures for DNFBPs were set out in Recommendation 24 while Recommendation 25 states that the competent authorities should establish guidelines, and provide feedback which will assist FIs and DNFBPs in applying national measures to combat ML and FT, especially in detecting and reporting suspicious transactions.

Regarding suspicious transaction reports Recommendation 16 states:

> *The requirements set out in Recommendations 13 to 15 and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:*
>
> *(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial*

---

[39] IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

> *transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.*
> *(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.*
> *(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).*
>
> *Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.*

2.3.7 Suspicious transactions

A suspicious transaction is any complex, unusual large transaction and all unusual patterns of transactions, without apparent economic or visible lawful purpose as defined in FATF Recommendation 11 essential criteria 11.1.

> *Financial institutions should be required to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.*

These transactions may represent proceeds of crime and it could involve money laundering and/or terrorist financing. The following are some general signs of suspicious transactions[40].

(Banks + DNFBPs)

- Assets withdrawn immediately after they are credited into an account.
- A dormant account suddenly becomes active without any plausible reason.
- The high asset value of a client is not compatible with either the information concerning the client or the relevant business.
- A client provides false or doctored information or refuses to communicate required information to the bank.
- The arrangement of a transaction either insinuates an unlawful purpose, is economically illogical or unidentifiable.

(Insurance Companies)

- Unusual or disadvantageous early redemption of an insurance policy;
- Unusual employment of an intermediary in the course of some usual transaction or financial activity (e.g. payment of claims or high commission to an unusual intermediary);
- Unusual payment method; and

---

[40] WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: pp. VI-18 – VI-24

- Transactions involving jurisdictions with lax regulatory instruments regarding money laundering and/or terrorist financing.

Signs regarding suspicious *cash transactions* are summarized below:

- Frequent deposit of cash incompatible with the information concerning either the client or his business.
- Deposit of cash immediately followed by the issuance of checks or transfers towards accounts opened in other banks located in the same country or abroad.
- Frequent cash withdrawal without any obvious connection with the client's business.
- Frequent exchange of notes of high denomination for smaller denominations or against another currency.
- Cashing checks, including travelers' checks, for large amounts.
- Frequent cash transactions for amounts just below the level where identification or reporting by the financial institution is required.

Signs regarding *transactions on deposit accounts* are as follows:

- Closing of an account followed by the opening of new accounts in the same name or by members of the client's family.
- Purchase of stocks and shares with funds that have been transferred from abroad or just after cash deposit on the account.
- Illogical structures (numerous accounts, frequent transfers between accounts).
- Granting of guarantees (pledges, bonds) without any obvious reason.
- Transfer in favor of other banks without any indication of the beneficiary.
- Unexpected repayment, without a convincing explanation, of a delinquent loan.
- Deposit of checks of large amount incompatible with the information concerning either the client or the relevant business.

2.4 Suspicious transaction reporting/report (STR)

Special attention should be paid to unusual patterns of transactions and complex and unusual large transactions[41]. These transactions should be examined thoroughly and the findings should be recorded systematically. Financial institutions should record the following information for each and every transaction and keep the records for a minimum of five years following the termination of the account[42].

- Name of the customer and/or beneficiary;
- Address;
- Date and nature of the transaction;
- Type and amount of currency involved in the transaction;
- Type and identifying number of account; and
- Other relevant information typically recorded by the financial institution.

If the findings are not satisfactory, the financial institution should consider declining the business and/or making a suspicious transaction report.

---

41 FATF Recommendation 11

42 FATF Recommendation 10

Recommendation 13 reads:

> *If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).*

In addition, Special Recommendation IV states:

> *If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorists organizations, they should be required to report promptly their suspicions to the competent authorities.*

Countries are encouraged to develop modern and secure techniques of money management providing accurate and complete record-keeping. These modern money management and payment methods, therefore, are very helpful to competent authorities and less vulnerable to money laundering.

Each jurisdiction has its own reporting threshold amount of money for each transaction established by a statute depending on its own circumstances. Financial institutions should be required to undertake customer due diligence (CDD) measures for any cash transaction that exceeds the threshold amount. On the other hand, certain entities that are assumed to be crime-free, such as government agencies, designated financial institutions and established businesses[43] make frequent, large transactions due to the nature of their businesses. They represent a low risk for engaging in money laundering and they may be eligible for exemption, but should be reviewed on a regular basis.

In order to avoid detection, criminals and terrorists use the method known as "smurfing" or "structuring" – multiple transactions below the national threshold using multiple accounts or a single account. Therefore, even a single transaction just below the threshold can be considered suspicious. With respect to multiple transactions, if the total transaction amount exceeds the threshold, the financial institutions need to report the entire series of transactions. Dealers in precious metals and stones are required to file STRs only when they engage in cash transactions with a customer equal to or exceeding the USD/EUR 15,000 threshold. It is one type of risk-based non-financial business and profession.

The reporting of suspicious transactions and cash transactions or the disclosure of records by a financial institution to a competent authority must be confidential under a country's bank secrecy laws. For combating money laundering and financing of terrorism purposes, Recommendations 4 and 8 encourage the countries to make appropriate exceptions in their bank secrecy or privacy laws but confidentiality must be observed.

---

[43] IMF and WB , Financial Intelligence Units: An Overview, 2004: p.50

The report on the AML-CFT assessments[44] by the IMF and the WB states:

> *For suspicious transaction reporting (STR) (Recommendation 13), only 6 percent were considered compliant, 22 percent largely compliant, 33 percent partially compliant, and 39 percent non-compliant.*

It also states:

> *61 percent of assessed countries were non-compliant with the FATF Recommendation (SR IV) that compels reporting of transactions when there is suspicion that there are funds linked to terrorism.*

3 Financial intelligence unit (FIU)

Countering money laundering effectively requires knowledge of banking, finance, accounting and other related economic activities in addition to that of laws and regulations, investigation and analysis. There may be insurmountable obstacles not only to obtaining the information from financial institutions but also to rapid exchanges of information with foreign counterparts without the assistance of a financial intelligence unit that provides the possibility of rapid exchange of information between financial institutions and law enforcement/prosecutorial authorities, as well as among jurisdictions.

In the simplest form, a financial intelligence unit (FIU) – a central agency to receive, analyze, and disseminate financial information to combat money laundering and terrorist financing – serves as a crucial element in an AML-CFT program to provide for the exchange of information between financial institutions and law enforcement agencies.

According to the Egmont Group's definition[45],

> *A central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:*
> *(i) concerning suspected proceeds of crime, or*
> *(ii) required by national legislation or regulation, in order to counter money laundering*

The following diagram[46] of the basic FIU concept shows that efficient FIUs provide assistance in exchanging information between financial institutions and law enforcement / prosecutorial authorities and between jurisdictions.

---

44 IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

45 The Egmont, Information Paper on Financial Intelligence Units and the Egmont Group http://www.egmontgroup.org/info_paper_final_092003.pdf, (December 2006)

46 ibid.: (December 2006)

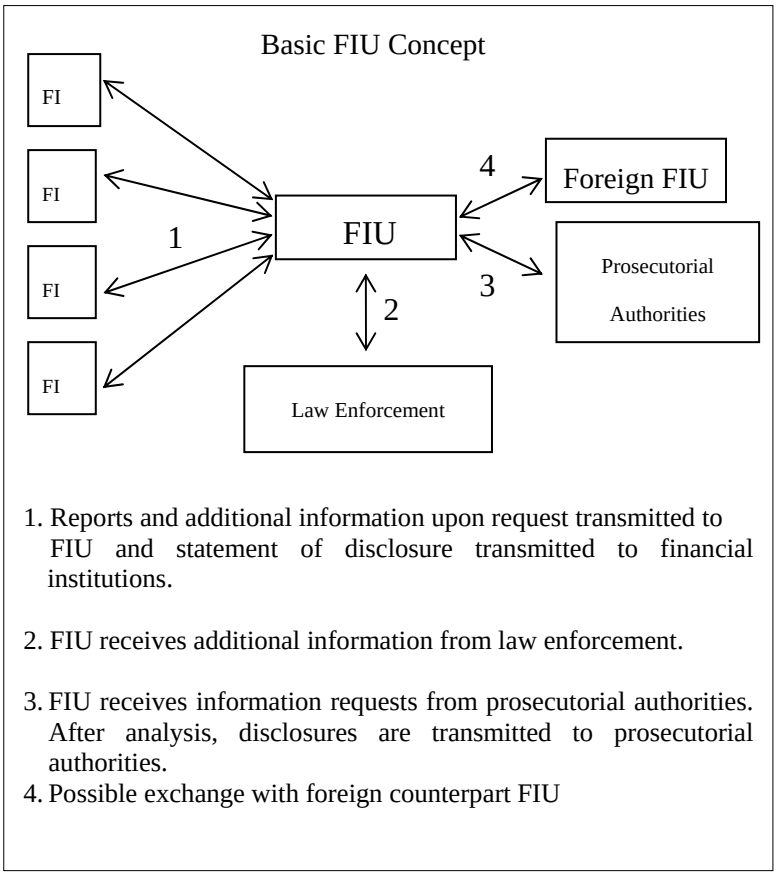

Figure 3: Showing basic FIU concept

3.1 Types of FIU

The basic features of an FIU should be consistent with the supervisory framework of that particular country as well as its legal and administrative systems and its financial and technical capabilities. The four basic FIU models recognized by the Egmont Group are Law Enforcement Model, Judicial Model, Administrative Model and Hybrid-Administrative Model[47].

- ***Law Enforcement-type FIUs***: Authorities that implement anti-money laundering measures alongside already existing law enforcement systems, supporting the efforts of multiple law enforcement agencies or judicial authorities with concurrent or sometimes competing jurisdictional authority to investigate money laundering.

- ***Judicial or Prosecutorial-type FIUs*** : The judicial model is established within the judicial branch of government wherein "disclosures" of suspicious financial activity are received by the investigative agencies of a country from its financial sector such that the judiciary powers can be brought into play e.g. seizing funds, freezing accounts, conducting interrogations, detaining people, conducting searches, etc.

---

47 The Egmont, Information Paper on Financial Intelligence Units and the Egmont Group http://www.egmontgroup.org/info_paper_final_092003.pdf, (2006)

- ***Administrative-type FIUs***: Centralized, independent, administrative authorities that receive and process information from the financial sector and transmit disclosures to judicial or law enforcement authorities for prosecution. That type of FIU functions as a "buffer" between the financial and the law enforcement communities.

- ***Mixed or Hybrid FIUs***: The hybrid model serves as a disclosure intermediary and a link to both judicial and law enforcement authorities. It combines elements of at least two of the FIU models.

3.2 Structure of FIU

The possible structure of a typical FIU is shown in the following Figure[48]

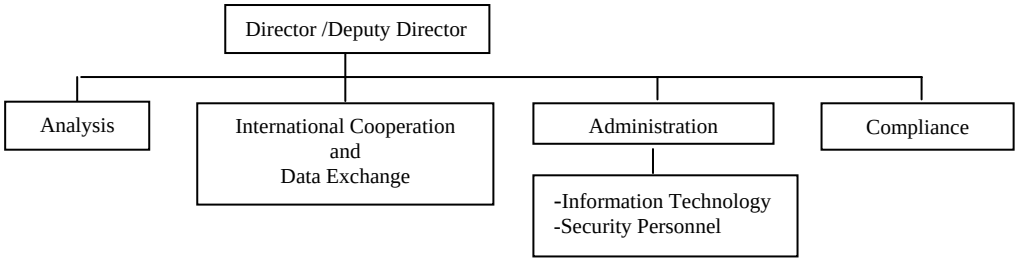

Figure 4: Showing structure of a typical FIU

The internal organization of an FIU varies depending on its functions and size. A sound internal organization is essential to efficiency and success. Most FIUs have analysis departments which are the key departments that receive and analyze the suspicious transaction reports. The department for international cooperation and data exchange – authorized to communicate directly with counterpart FIUs and other foreign bodies– usually covers multilateral and bilateral cooperation matters. If an FIU reaches a certain size it should have a department of administration to supervise the compliance of reporting entities with AML-CFT requirements. The department of compliance that carries out regulatory and supervisory functions monitors compliance with AML-CFT requirements and initiates the sanctions mechanism in case of serious failures to report transactions. Since information technology facilitates the work of the FIU organizations the maintenance of the supporting computing infrastructure becomes a vital component of the FIUs' operations. The department of information technology and security personnel takes care of this matter.

3.3 Core functions

The Egmont Group formalized the definition of FIU based on 3 core functions[49] regarding money laundering and terrorist financing in 1996. Similar definitions have been incorporated in the 2004 FATF Recommendations and in the two UN international conventions – the Palermo Convention and the Convention against Corruption.

---

[48] IMF and WB Group, "Financial Intelligence Units :An Overview", (2004): p. 28

[49] ibid.: p. 33

3.3.1 Receiving information

The first core function is receiving information from the following sources.

The first source is from the financial institutions. Banking systems through which great amounts of money can be transmitted likely become focal points for financial misuse. Besides, not only the banking system is vulnerable to ML due to its ability to move funds rapidly, but also insurance companies and securities firms are also vulnerable to ML because of the variety of services that can be used to conceal the sources. Reports of financial institutions, therefore, are the most important data to be received by FIUs. Financial institutions have to know their obligations and are encouraged to provide necessary information to the authorities concerned. Otherwise, they are reluctant to provide the information for not to loose customers and in the long run, they will not have any concern about the results of ML related transactions that will affect the reputation of financial institutions. They also have to know that there is no more anonymous account and the information must be made available for law enforcement agencies and judges.

The second source is non-financial institutions. Criminals' use of non-financial institutions – casinos, lawyers, notaries, other independent professionals, accountants, trust and company service providers, and dealers in precious metals and stones – should not be ignored. They may attempt to use non-financial institutions which have less sophisticated systems to detect money laundering crimes than financial institutions. Non-financial institutions should also know their obligations and should be given necessary guidance relating to AML-CFT matters.

Accordingly, FIUs have to receive STRs from both financial institutions and non-financial institutions.

The third source is an entity concerned that reports transactions suspected of being related to terrorism. Almost all counties have implemented the FATF Special Recommendations (except SR IX which was issued on 22 October 2004) by amending the law in which the reporting obligation is contained.

Fourthly, large-scale transactions – above the threshold amount – are to be reported[50].

Finally, reports of cross-border transportation of currency and bearer negotiable instruments take an important role in fighting money laundering and terrorist financing. The customs authorities are required to report to the FIU. One of the most important obligations of an FIU, under the first core function "receiving information" is the exchange of financial data and intelligence with other FIUs[51]. FIUs are to receive suspicious transaction reports and data from other FIUs. In some countries, an FIU is responsible to decide the form and contents of reports. The reports can be filed in paper forms or electronically depending on the circumstances. In most cases, the report includes the particulars of the transaction and the customer, and the reason(s) why the transaction is considered suspicious.

---

50 The 2004 FATF Recommendation 19

51 Egmont, Annex to the Egmont Group "Statement of Purpose", http://www.egmontgroup.org/princ_info_exchange.pdf

3.3.2 Analyzing the information

The analysis of reports received from reporting entities is the second core function of an FIU. If the number of reports is too large for the FIU to be able to analyze all of them in time, the FIU may use internal criteria to prioritize reports and deal only with the most important ones. After collecting additional related information for a particular case, the process goes through different stages of analysis and ends with the result – a detailed file concerning an ML/FT case. The file is forwarded to one of the three destinations: (1) the law enforcement authorities; (2) the prosecutors; and (3) the reaching of a conclusion that no suspicious activity was found.

There are three levels of analysis: tactical analysis, operational analysis and strategic analysis. They are defined[52] as follows:

> *Tactical analysis is the process of collecting data needed to build up a case establishing wrong-doing and accompanying facts that clarify the reasons behind the commission of a criminal offense.*
>
> *Operational analysis consists of using tactical information to formulate different hypothesis on the possible activities of the suspect to produce operational intelligence.*
>
> *Strategic analysis is the process of developing knowledge ("strategic intelligence") to be used in shaping the work of the FIU in the future. The main characteristic of strategic intelligence is that it is not related to individual cases, but rather to new issues and trends.*

3.3.3 Disseminating the information

The third core function of an FIU is the dissemination of the received information and sharing of the analysis domestically and internationally. Rapid dissemination and sharing of information or reliable financial intelligence is extremely important for the effectiveness of national AML-CFT regime and its ability to cooperate internationally. There are 3 aspects to the dissemination function[53]:

1. Transmitting reports for investigation or prosecution.
2. Sharing information with other domestic agencies and requesting information from an FIU.
3. International information sharing
   - Legal basis for exchange of information between FIUs
   - Exchange of information
   - Special arrangements for terrorist financing cases
   - Egmont Group principles of information exchange in money laundering cases

3.4 Additional non-core functions

In addition to the three core functions, FIUs are also entrusted with additional non-core functions. They are:

---

[52] IMF and WB, Financial Intelligence Units: An Overview, 2004: pp. 57 – 61

[53] ibid.: pp. 61 – 70

- Monitor the compliance of certain entities with AML-CFT rules and standards
- Block reported suspicious transactions for limited time
- Train reporting-entity staff on reporting and other AML-CFT obligations
- Conduct research
- Enhance public awareness

Financial institutions have their own bank secrecy laws and the criminal justice system has laws against money laundering and terrorist financing. There may be a policy tension between these two frameworks of laws. FIUs, intermediaries between the reporting entities and the criminal justice system, are required to exert their power to reduce the tension between privacy and efficiency. Recommendation 4 helps FIUs to push against the extreme limits of financial privacy laws, raising legitimate concerns about the potential for the abuse. It states:

> *Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.*

In addition, Principle 7 of the Egmont Group's Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorist Financing Cases (the Egmont Group 2001) states:

> *FIUs should work to encourage that national legal standards and privacy laws are not conceived so as to inhibit the exchange of information, in accordance with these principles, between or among FIUs.*

FIUs that take a crucial role in AML-CFT regimes need to be vigilant as they are repositories and guardians of highly sensitive information relating to the crime of money laundering and terrorist financing. Confidentiality is one factor to institute stringent procedural safeguards for their important financial evidence gathering and information sharing functions.

Confidentiality requirements should be drafted according to Principle 13 of the Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorist Financing Cases (the Egmont Group 2001) that states:

> *All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner consistent with national provisions on privacy and data collection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.*

Independence and accountability support the trust between the reporting entities and the justice system. FIUs should be independent from political influence and other supervisory bodies regarding analysis of cases and dissemination of the resulting financial intelligence. At the same time, there should be a certain measure of accountability that is essential for the three core functions, but FIUs should not be influenced by other government authorities.

It is important for FIUs to give back general information to financial institutions about their reports. FIUs need to give back general feedback to reporting entities about the

usefulness of their reports as well as suggestions on how to improve their way of reporting suspicious transactions. FIUs should share the information about money laundering and terrorist financing trends and typologies with reporting entities. Recommendation 25 states:

> *The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.*

FIUs should maintain comprehensive statistics on STRs received, analyzed and disseminated for further reference in AML-CFT assessments. Recommendation 32 states:

> *Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.*

4 International cooperation

International cooperation is needed at all stages of AML-CFT procedures especially in obtaining information related to money laundering and terrorist financing from abroad as preventive measures. All of the three conventions - the Vienna Convention (1988), the Convention against FOT and the Palermo Convention – and the 2004 FATF 40+9 Recommendations give explicit recognition to the fact that international cooperation should be supported by a network of mutual assistance. Laws and procedures should, therefore, encourage and facilitate mutual legal assistance in obtaining evidence for use in AML-CFT investigations and prosecutions. FATF Recommendation 36 states:

> *Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:*
>
> *(a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.*
> *(b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.*
> *(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offense is also considered to involve fiscal matters.*
> *(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.*
>
> *Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign*

> *judicial or law enforcement authorities to domestic counterparts.*
>
> *To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country."*

Special Recommendation V also reads:

> *Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquires and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.*
>
> *Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organizations and should have procedures in place to extradite, where possible, such individuals.*

4.1 Effective international cooperation mechanism

The UN has been used as a place for leaders of the countries to speak freely of their grievances since the end of World War II. It has evolved as things have changed and different types of problems have emerged. Currently we have problems of money laundering and international terrorism. A country has to identify priorities, build up its efficient domestic capacity, and determine the means for combating ML and FT taking into account its economic and environmental needs. A country's capacity-building depends on its people and institutions, technological capabilities, ecological and geographical conditions and so forth. In order to strengthen international cooperation, endogenous capacity is essential and the efforts of the countries in partnership with relevant UN organizations are required to obtain endogenous capacity.

In order to construct an effective international cooperation, countries should meet three prerequisites[54]. They are:

1. Building a comprehensive and efficient domestic capacity.
2. Ratifying and implementing the international conventions.
3. Complying with the FATF Recommendations and other sector-specific international standards.

All necessary administrative and supervisory authorities as well as an FIU with necessary powers and responsibilities should be in place adequately provided with staff, budget and other useful resources to carry out their duties efficiently[55], especially to oversee financial institutions. In addition, criminal justice system and judicial/prosecutorial system are two crucial factors to obtain an effective AML-CFT regime.

---

[54] WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p. VIII-2

[55] FATF Recommendation 30

Having established an effective AML-CFT regime, countries need to sign and ratify the relevant international conventions, especially the three conventions – the Vienna Convention (1988), the Convention against Financing of Terrorism (1999) and the Palermo Convention (2000). It is also necessary to sign and ratify the other AML-CFT conventions adopted by their respective regional organizations. All provisions of the aforementioned conventions should be fully implemented in their domestic laws. Provisions related to the criminalization of money laundering and international cooperation will help the countries obtain effective international assistance.

In order to obtain complementary effectiveness, apart from the international conventions, countries should comply with international standards. In particular, emphasis should be placed on the FATF 40+9 Recommendations; the Core Principles (the Basel Committee); Customer Due Diligence (the Basel Committee); the Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorist Financing Cases (the Egmont Group 2001); and other international standards set by the IAIS and the IOSCO.

4.2 Fundamentals of international cooperation mechanism

Money laundering and international terrorism remains a great threat to peace and security in the world today and all governments, particularly the major powers, need to strengthen anti-money laundering and counter-terrorism cooperation internationally, regionally, and bilaterally to overcome the common and growing threat of international terrorism.

According to the international conventions and standards, the following principles are prominent[56].

1. When competent authorities in one country officially request those in another to provide the information relating to money laundering and terrorist financing obtained by the latter, the requested authorities should provide the information promptly to the requesting authorities.
2. When competent authorities in one country officially request assistance on the sole ground that the request is also considered to involve fiscal matters, the requested authorities should not refuse the request for assistance.
3. When competent authorities in one country know that certain information would be useful to those in another country the former should provide the information spontaneously to the latter without being asked.
4. Competent authorities in one country should be able to conduct inquiries and investigations, and perform other requested actions on behalf of its foreign counterparts.

The following points[57] are essential to obtain effective international cooperation between law enforcement agencies and judicial authorities.

1. Countries should sign, ratify and implement all the relevant conventions[58] conducted by the UN and regional international organizations as they provide

---

[56] FATF Recommendation 40

[57] WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: pp. VIII-11 – VIII-13

[58] FATF Recommendation 35

necessary legal basis for international cooperation.

2. Effective laws and clear and efficient procedures should encourage and facilitate mutual legal assistance[59]in AML-CFT matters.
3. Competent authorities must provide appropriate assistance in relation to money laundering and terrorist financing to the foreign counterparts for (1) the production of information; (2) searches of financial institutions; (3) the taking of witnesses' statements; and (4) the tracking, identifying, freezing, seizure, and confiscation of assets laundered or intended to be laundered, the proceeds of money laundering and assets of corresponding value[60].
4. Treaties or other formal arrangements and informal mechanisms must be in place to support international cooperation via bilateral or multilateral mutual legal assistance.
5. Laws and procedures should allow for the extradition of the accused without undue delay[61].
6. National authorities should keep both statistical and factual records for information exchange between countries.

4.3 Role of FIUs in international cooperation

Since FIUs are organized with the major purpose of combating money laundering and terrorist financing, and they have common features and act in accordance with the Egmont Group's principles, FIU cooperation at the international level is very important. When dealing with international requests for information, the Egmont Group provides guidelines in terms of best practices for the exchange of information between FIUs. Regarding international cooperation between FIUs, there are three factors to be focused on: (1) the core features of FIU international cooperation; (2) conditioning the FIUs' abilities to cooperate at the international level; and (3) the relationship between different organizational modals and international cooperation. An FIU, mostly attached to administrative authorities, should cooperate with all its counterparts regardless of their internal and organizational structure. However, three important points should be considered[62]. They are:

1. Whether there are or should be restrictions on sharing financial information;
2. If so, how much information should be shared; and
3. What type of information should be shared.

4.4 Financial institutions and DNFBPs

As most money laundering activities have been with the banking system, financial supervisors are authorized to cooperate with their counterparts with respect to AML-CFT analysis and regulatory investigation. The Basel Committee issued the twenty five Core Principles (1997) for applying to all banking supervisors. In particular Principles 23, 24 and 25 state the issues regarding international cooperation. The Committee also issued Core Principles Methodology (1999) that describes under what conditions assessments should be made and detailed explanation of each principle.

---

59 FATF Recommendation 36
60 FATF Recommendation 38
61 FATF Recommendation 40
62 WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p. VIII-8

Recommendations 4 and 40 also support the point that countries should not use the financial institution secrecy law as a ground for refusing to provide the mutual legal assistance and extradition. Recommendations 35-40 deal with international cooperation regarding AML-CFT for financial institutions and DNFBPs.

Although a country (home country) can establish a branch of its bank in another country (host country) using informal or formal arrangements for a proper information sharing system, the home country supervisor has to close the bank if the host country does not have an adequate supervision of the bank relative to the risk management[63]. The home country supervisors are required to exchange information with the host country supervisors[64] regularly so that the home country supervisors have up-to-date information at their fingertips. As financial institutions and DNFBPs have taken the vital roles in the AML-CFT process, prompt and efficient assistance and cooperation done by supervisors of those institutions can produce the fruitful result in any AML-CFT regime.

4.5 Insurance companies

Cooperation between insurance supervisors is another support in detecting cases related to money laundering and financing of terrorism. The International Association of Insurance Supervisors is committed not only to setting out the principles that are fundamental to effective insurance supervision but also to developing standards, including the principles relating to international cooperation, that can be used by the insurance supervisors throughout the world as efficient and timely exchange of information is critical to the effective supervision in international insurance sector and essential for the effective supervision of the financial system. Principles can be implemented in a flexible manner depending on the circumstances of a particular jurisdiction.

Insurance Core Principle (ICP) 5 is described in ten essential criteria[65] for supervisory cooperation and information sharing. ICP 5 reads:

> *The supervisory authority cooperates and shares information with other relevant supervisors subject to confidentiality.*

In most IAIS member countries money laundering and terrorist financing are criminal acts under the law. In conjunction with law enforcement authorities and in cooperation with other supervisors, insurance supervisors should supervise insurers and intermediaries for AML-CFT purpose. ICP 28 states:

> *The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to take effective measures to deter, detect and report money laundering and financing of terrorism consistent with the Financial Action Task Force on Money Laundering (FATF).*

---

63 Basel Committee on Banking Supervision, Core Principles Methodology April 2006: Core Principle 23 essential criterion 2, p. 37

64 ibid.: Core Principle 24 additional criterion 2, p.38

65 IAIS, Insurance Core Principles and Methodology, October 2003 http://www.insurance.gov.gy/Documents/IAIS%20Core%20Principles.pdf

ICP 28, criterion (c) explains:

> *The supervisory authority has appropriate authority to cooperate effectively with the domestic Financial Intelligence Unit (FIU) and domestic enforcement authorities, as well as with other supervisors both domestic and foreign, for AML-CFT purpose.*

The exchange of information between supervisory authorities is a key element in pursuing insurance activities on the Internet. The IAIS consequently issued the Principles on the Supervision of Insurance Activities on the Internet in October 2004, where Principle 3 states:

> *Supervisors should cooperate with one another, as necessary, in supervising insurance activities on the internet.*

4.6 Securities firms

Cooperation between supervisory authorities of securities firms should be in place at the international level to facilitate the detection and deterrence of money laundering and terrorist financing cases. The international Organization of Securities Commissioners issued Resolutions on Money Laundering in October 1992, where Resolution 7 states:

> *Each IOSCO member should consider the most appropriate means, given their particular national authorities and powers, to share information in order to combat money laundering.*

In addition, the IOSCO Core Principles 11, 12 and 13 encourage the regulators to have an adequate information-sharing arrangement with regulators in other countries.
Although competent authorities should provide the widest possible range of international cooperation to their foreign counterparts, certain limitation of conditions can be placed on their assistance. If a country does not criminalize certain fiscal offenses, it may not be able to provide assistance in connection with money laundering of the proceeds of a fiscal crime to the requesting country.

International cooperation between law enforcement agencies and judicial authorities is vital to achieve the goals of any AML-CFT regimes. Recommendations 36 to 40 and Special Recommendation V encourage the countries to provide the widest possible range of mutual assistance on the basis of a treaty, arrangement or other mechanism for mutual legal assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings in relation to money laundering and terrorist financing.

5 Combating money laundering and terrorist financing

5.1 Effective legal framework

Mainly based on the UN international conventions, the 2004 FATF 40 Recommendations and 9 Special Recommendations were created and it is unquestionable that they are invaluable to law enforcement and judicial authorities in AML-CFT regimes. Therefore, the first step of the AML-CFT process is to ratify and implement the UN conventions or UN instrumentalities. In particular, implementation

of the Vienna Convention (1988), the Convention against Financing of Terrorism (1999) and the Palermo Convention (2000) is essential to obtain an effective AML-CFT regime in accordance with the FATF Recommendations. Apart from the UN conventions, countries should fully ratify and implement the AML-CFT conventions adopted by their respective regional organizations. Besides the aforementioned conventions, countries should fully implement UN Resolutions dealing with terrorist financing, especially United Nations Securities Council Resolution 1373[66].

Under Recommendation 3, concerning ML, countries are encouraged to adopt measures similar to those set forth in the Vienna and Palermo Conventions and such measures should include:

(a) Identifying, tracing and evaluating property which is subject to confiscation;
(b) Carrying out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property;
(c) Taking steps that will prevent or void actions that prejudice the State's ability to recover property alleged to be liable to confiscation; and
(d) Taking any appropriate investigative measures.

Although Recommendation 3 covers terrorist financing cases as money laundering predicate offenses, Special Recommendation III emphasizes freezing and confiscating of terrorist assets.

> *Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.*
>
> *Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations.*

5.2 Countermeasures against ML and FT

In order to have a comprehensive legal and institutional framework for AML/CFT, domestic laws should be modified, adjusted and amended in line with the related international conventions and UN resolutions. First of all it is essential to criminalize money laundering and financing of terrorism. Second, institutional arrangements for AML/CFT should be made. Third, it is also essential to provide an adequate framework of extensive measures for prevention and detection of money laundering and terrorist financing. Fourth, there should be measures to control the proceeds of crime efficiently.

Since banks are the financial institutions used by money launderers and criminals, a Bank Secrecy Act is one of the legal actions. If there is a secrecy law in the banking system that obstructs cooperation and provision of information needed for investigation of money laundering and terrorist financing offenses a Bank Secrecy Act

[66] FATF Special Recommendation I

– which would provide law enforcement authorities with a tool to facilitate investigations into the criminals' financial activities to monitor domestic and international money flows and identify potential launderers – is needed.

Countries have modified their respective Bank Secrecy Act to prevent banks and other financial service providers from being used as intermediaries for criminal activities or to hide the transfer or deposit of money derived therefrom.

The fixing of a threshold level amount makes the money launderers hesitate to use large-scale cash transactions. They create a new process known as "smurfing"– splitting of a large amount of money into multiple smaller transactions. Multiple smaller transactions are less noticeable and it is easy to evade the bank reporting requirements. Even though the amount of currency is above the threshold level, most banks simply ignore the rules. In spite of heavy penalties for reporting violations, banks are not eager to abandon the source containing considerable revenue. The Bank Secrecy Act, therefore, is amended to impose much heavier penalties for reporting violations. Banks need to educate their employees how to carry out the KYC/CDD process so that they know their customers properly as numerous crimes including foreign crimes have been carried out using banks by money launderers and criminals.

The anti-money laundering acts in different countries are passed to combat money laundering. Banks are forced to obtain statements from the customers who are exempted, and banks are exempted from penalties under financial privacy laws when reporting suspicious transactions. Consequently, fees paid for money laundering have risen dramatically and financial institutions cannot control their temptation. Accordingly, several of them are fined for money laundering. Adequate administration and supervision of financial institutions, especially for suspicious transaction reports, is critical in combating ML and FT.

In addition, fighting against corruption is one means of countermeasures because corruption at the highest levels of government is one type of catalyst for the success of the money laundering process. There are different types of factors which can be used to facilitate performing money laundering but they are hindrances to combating money laundering. Whatever the obstacles there are in anti-money laundering and counter-terrorist financing, it is essential that the financial institutions must act in partnership with law enforcement and supervisory authorities in order to get rid of the obstacles in combating the twin evils. The alarming fact for the international community is that terrorist financing submerged under the money laundering process is a transnational movement of funds by using many countries whose governments firmly believe in absolute financial privacy.

5.3 Effective implementation

In addition to the adoption of laws, regulations and other measures, effective implementation is required to strengthen the AML-CFT regime. In some countries, despite the adoption of AML-CFT laws, implementation of the adopted laws is weak. Countries have to implement and utilize the appropriate laws, regulations and other measures that have been adopted. Effective implementation in the initial stages of AML/CFT enforcement - the most important part of the implementation – is critical. Without suspicious transaction reports, viable and effective investigation, and good control of the proceeds of crime, it is obviously hard to achieve justice in prosecution.

5.3.1 Suspicious transaction reporting/report

One of the most effective and helpful factors in combating ML and FT is reporting suspicious transactions. Financial institutions should promptly report their suspicious transactions that are linked to money laundering or terrorism to the respective competent authorities. The reporting requirements must be in accordance with that particular country's AML-CFT laws.

Recommendations 13, 14, 16 and 26 deal with ML-related suspicious transaction reports regarding financial institutions, DNFBPs and competent authorities respectively whereas Special Recommendation IV deals with terrorism-related suspicious transaction reports. Recommendation 32 encourages competent authorities to maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of such system for further reference.

5.3.2 Investigation of ML-FT offenses

Although many countries have adopted money-laundering laws around the world, vigorous enforcement is limited to a few countries. Money-laundering techniques develop constantly and money-laundering is said to be the world's third largest business by value[67]. Investigative techniques tend to have some loopholes because laundered money can still be moved around the world. It is therefore extremely important for investigators to obtain the fundamental knowledge and necessary skills about money-laundering investigations and continuously follow the latest money-laundering typologies. More importantly, investigators should be provided with adequate, advanced technological facilities for the use in their daily operations, and training opportunities to strengthen their professional investigative capacity. In this regard, countries with advanced knowledge and skills in the ML investigation should provide technical assistance to countries with weak institutional capacity.

5.3.3 Control of the proceeds of crime

The most effective measures against ML-FT are tracing, freezing, seizing and confiscating the proceeds of crime so that the volume of dirty money business and financial support to terrorists can be reduced. Consequently, domestic and international efforts to further develop and utilize those measures should be enhanced using proper mechanisms.

5.4 Knowledge of untraceable ML-FT methods

In combating money laundering and terrorist financing, untraceable means of money/value transfer should be seriously considered. Having known that these methods have been used by money launderers and terrorist organizations, authorities should take some kinds of measures to impose AML-CFT requirements on the money/value transfer systems in AML-CFT regimes. The competent authorities of AML-CFT regimes have established guidelines that assist financial institutions and

---

[67] David Lyman (Senior Partner Tilleke & Gibbins Rev.), Money Laundering, Thailand English Language Law Forum, February 17, 1999 http://www.thailawforum.com/articles/moneylaunderingtg.html [Read December 2006]

designated non-financial businesses and professions in applying national measures to combat money laundering and financing of terrorism, providing training courses and seminars in connection with the ML-FT methods. There are some types of money laundering methods apart from the ones mentioned in Chapter 2, (1.4). Some money launderers use informal money remittance systems without being supervised. The most alarming methods that hinder combating ML and FT are alternative remittance systems, wire transfers, misuses of non-profit organizations and cross-border transactions.

Terrorists raise money from both legal and illegal activities. Charitable contributions can be major sources of funding via non-governmental organizations. Informal money transfer systems can be the method terrorists and terrorist organizations prefer to use for these methods do not leave traces for detection.

5.4.1 Alternative remittance systems

Alternative remittance systems – known as informal value transfer systems or underground banking systems – transfer value without using formal money remittance systems. In other words, an alternative remittance system is a type of financial service through which funds or values are transferred without being supervised. Trade-based money laundering can also be viewed as a type of alternative remittance system. Trade-based value transfers that are vulnerable to terrorist financing are commonplace in many parts of the world. The International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs (March 2004)[68] states:

> *In one example of how alert customers scrutiny stopped suspect trade goods with ties to terrorism, a European Customs service intercepted a shipment of transshipped toiletries and cosmetics that originated in Dubai. Customs examination of the manifest suggested that the goods were counterfeit and they were grossly undervalued. The goods were ultimately consigned to a third country. The resultant investigation revealed that the original exporter of the goods was a member of al-Qaida.*

One point should be pondered that it is impossible to eliminate the informal money value transfer systems because in some of the developing countries that method is the only viable means of transferring money. Even if some countries do have formal money remittance systems, the formal financial institutions provide the service at an inordinate price. The reason these alternative remittance systems are in demand and attractive to both criminals and legitimate customers is they are cheaper and faster than formal banking systems. Without this type of system people who cannot easily access the formal financial sector will have some inconvenience. On the other hand, taking this fact as an advantage, money launderers and terrorists have willingly used this method to transfer the fund from one place to another. It is extremely difficult to tackle the illegal informal remittance systems.

---

[68] US Department of State, The International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs, March 2004 http://www.state.gov/p/inl/rls/nrcrpt/2003/vol2/html/29910.htm [Read December 2006]

The final part of Recommendation 23 and Special Recommendation VI focus on informal alternative remittance systems. Special Recommendation VI encourages countries to impose AML-CFT requirements on forms of money move or value transfer systems and aims to apply AML-CFT controls to money launderers and terrorists who take advantage of alternative remittance systems.

5.4.2 Wire transfers

Money launderers have made extensive use of electronic payment and message systems or "wire transfers" where movement of funds without the identity of originator between accounts is a double click. As a result, investigations of major ML cases have become more difficult to pursue. The term "wire transfer" refers to any transaction of an amount of money through a financial services business by electronic means to a beneficiary at another financial services business, where the originator and the beneficiary may be the same person. In order to facilitate the investigations of money laundering cases, the FATF issued Special Recommendation VII.

> *Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.*
>
> *Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).*

Countries should take appropriate actions to require financial institutions to obtain accurate and meaningful information of the originator on wire transfers[69] where the threshold of wire transfers must not be above USD 3000[70] Full originator information contains:

- the name of the originator;
- the originator's account number (or a unique reference number if no account number exists); and
- the originator's address (Countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.).

In addition, beneficiary financial institutions should adopt effective risk-based procedures for handling wire transfers with incomplete originator information[71]. Regarding cross-border wire transfers, the transfers need to be accompanied by the name, account number and address of the originator[72]. If the account number does not exist, a unique reference number can be used. Domestic wire transfers need to be accompanied by the account number, only if the rest of the information about the

---

69 FATF Special Recommendation VII, essential criteria VII.1
70 ibid.: essential criteria VII.4
71 ibid.: essential criteria VII.7
72 ibid.: essential criteria VII.2

originator can be traced by authorities concerned within three business days[73].

5.4.3 Non-profit organizations

In general, non-profit organizations which enjoy tax exempt status as a result of being organized to serve the public interest. Nowadays, charities may be operating under great difficulty in different parts of the world where non-profit organizations are misused by terrorist financiers. In order to reduce the risk of non-profit organizations, the FATF has issued a set of international best practices entitled "Combating the Abuse of Non-profit Organizations: International Best Practices[74]". These guidelines inform non-profit organizations how activities should be carried out and how to prevent non-profit organizations from being misused to finance terrorism.

Under Special Recommendation VIII, a country should ensure that, its non-profit organizations cannot be used by terrorist organizations or for terrorist financing. It reads:

> *Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:*
> - *by terrorist organizations posing as legitimate ones;*
> - *to exploit legitimate entities as conduits for terrorist financing, including to avoid asset freezing measures; or*
> - *to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.*

In order to achieve the goals of Recommendation VIII, there are three requirements[75] for attention of countries. They are:

- *Ensure financial transparency*
- *Programmatic verification*
- *Administration*

5.4.4 Cross-border transactions

The FATF encourages countries to set the policies designed to tackle dirty money passing through the global system and the financing of terrorism as the banking systems become tightened. Consequently, money launderers and terrorist organizations have changed their way of laundering and financing. They choose the methods by which they can use cash without a trace and they have increasingly done so.

Special Recommendation IX states:

> *Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.*

---

73 FATF Special Recommendation VI, essential criteria VII.3

74 FATF, Combating the Abuse of Non-profit Organizations: International Best Practices, 11 October 2002, http://www.icnl.org/JOURNAL/vol5iss1/cr_int.htm [Read January 2007]

75 WB, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, second edition, 2004: p. IX-13

> *Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.*
>
> *Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.*

Under Special Recommendation IX, countries should have measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III[76], in place by implementing one or both of the following two types of systems for incoming and outgoing cross-border transportations of currency/bearer negotiable instruments[77].

(a) Declaration system

(i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments that are of a value exceeding a prescribed threshold should be required to submit a truthful declaration to the designated competent authorities; and
(ii) The prescribed threshold cannot exceed EUR/USD 15,000.

(b) Disclosure system

(i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments should be required to make a truthful disclosure to the designated competent authorities upon request; and
(ii) The designated competent authorities should have the authority to make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

Competent authorities should have the legal authority not only to request and obtain information from the couriers who make false declaration(s) or disclosure(s) of currency/bearer negotiable instruments or failure to declare/disclose them but also to stop or restrain currency/bearer negotiable instruments that are suspected to be related to money laundering and terrorist financing . Unusual or suspicious cross-border movements of currency, other negotiable instruments and highly valued commodities (precious stones/metals) should be reported to the country customs services or other appropriate authorities[78].

---

[76] FATF Special Recommendation IX, essential criteria IX.10 and IX.11
[77] ibid.: essential criterion IX.1
[78] FATF Recommendation 19

5.4.5 Use of false identity

In addition to the aforementioned three ML methods, there is another method – money laundering using false identity – that makes the authorities of financial institutions hard to see the actual picture of money transactions. Identity theft dealing with two activities [79] – acquiring, collecting and transferring personal information from a tangible source (an actual document) or an intangible source (a computer screen) and using the obtained information as an instrument of crime in future – has been used in transactions.

It is stated in the "Report of the Workshop Measures to Combat Economic Crime, Including Money-Laundering – Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005" that examples of the more common ways in which personal information is obtained for later criminal use are as follows:

1. *Theft of purses and wallets; theft of documents from the mail; redirection of mail from the victim's home to perpetrator's home;*
2. *Recovering from trash documentation that identifies personal information relating to the victim, for example, a credit card or bank account number (dumpster diving);*
3. *Unauthorized copying of digitized data (e.g. "skimming" devices that record credit card and/or debit card numbers; a hidden camera to record personal identification numbers (PIN) accompanying the skimming of debit cards);*
4. *Obtaining personal information in respect of a dead person in order to assume their identity (tombstoning)*
5. *Obtaining personal information from public sources (e.g. "shoulder surfing", which involves looking over someone's shoulder while they are entering their PIN when using a debit card);*
6. *Obtaining personal profile information on an individual from the Internet with a view to using that information to impersonate them;*
7. *Using the Internet to direct victims to a website that looks like that of a legitimate business. At the website the victim is asked to disclose his or her personal information. The personal information is collected by the criminal for later use to commit fraud or another form of economic crime (this activity is called "phishing");*
8. *Compromise of large databases (e.g. hacking into public or private computer databases to obtain personal information in order to make false identification documents); and*
9. *Using personal information supplied by corrupt government or company employees to make forged documents (e.g. false driver's licenses) or obtaining false identification documents from such employees.*

---

[79] UN Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, Ekobrottsmyndigheten Swedish National Economic Crimes Bureau, Report of the Workshop Measures to Combat Economic Crime, Including Money-Laundering – Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18-25 April 2005.

5.5 International cooperation in AML-CFT

As mentioned above, international cooperation deals with different areas such as financial institutions, DNFBPs, insurance companies, securities firms, etc.

As ML- and FT-related crimes have taken place increasingly across national borders it has been challenging investigative authorities to trace and prove complicated transnational money flow. In order to perform an effective investigation, international cooperation through the Egmont Group, facilitator among financial intelligence units around the world, is essential.

Countries should take appropriate measures to ensure that they do not provide safe havens for terrorists and money launderers. Apart from national countermeasures, regarding international cooperation in combating money laundering and terrorist financing, Recommendations 35 to 40 and Special Recommendation V provide that each country should cooperate with another country through a mutual legal assistance mechanism or other mechanisms.

5.6 Technical assistance in AML-CFT

Regardless of country income level, the establishment of viable AML-CFT regimes requires significant expenditure to develop appropriate institutions, recruit personnel, train staff and acquire advanced technology. Technical assistance (TA) is one factor to facilitate the establishment and development of efficient and effective AML-CFT regimes by developing countries that need expertise and knowledge, up-to-date information and other resources necessary for the process. The World Bank and the International Monetary Fund, in cooperation with the Financial Action Task Force, the FATF-style regional bodies, the UN Global Program against Money Laundering and other key organizations and national governments are involved in combating money laundering and terrorist financing. TA donors and providers are encouraged to respond to TA requests related to combating the financing of terrorism on a priority basis.

In order to meet the major objective of TA, to assist countries in the implementation of the full AML-CFT standard, TA includes[80]:

- Designing institutional framework;
- Legislative drafting and provision of legal advice;
- Enhancing financial supervisory regimes;
- Building capacity of financial intelligence units and other agencies;
- Traditional workshops and seminars;
- Videoconferencing (Global Policy Dialogues);
- Multi-year (Capacity Enhancement Program);
- Appointment of mentors and peripatetic advisors; and
- Publications on a wide range of AML-CFT topics.

Technical assistance can be research and information exchange; needs analysis; consultancies and advisory services; study tours; awareness-raising seminars;

---

[80] IMF and WB, Anti-Money Laundering and Combating the Financing of Terrorism: Observations from the Work Program and Implications Going Forward, Supplementary Information, 31 August 2005, http://www.imf.org/external/np/pp/eng/2005/083105.pdf [Read November 2006]

development of model laws and regulations; assistance in drafting legislation and regulations; local, national or regional training courses; computer-based training modules; mentoring and attachments; guidance notes and best practice tools; and communication and information technology support and training.

Effective technical assistance programs require mechanisms and projects that are flexible and appropriate to the identified needs of the requesting country. One of the requirements of an efficient approach to combat ML-FT is to deliver sequential technical assistance across several sectors, including awareness raising and policy development of measures relevant to the regulatory and financial sectors. It is also required to provide assistance to support law enforcement processes.

It is needless to say that solid foundation for effectively sequencing and coordinating the delivery of technical assistance by identifying with accuracy; the relevant technical assistance and training needs compiled from a wide variety of sources and frameworks – bilateral and multilateral needs assessment studies and missions; compliance assessments and mutual evaluations in relation to relevant global standards; self-assessments; and country statements in the context of regional and international forums are crucial in combating ML and FT.

6 Chapter-wise comments

There are some challenges in combating ML-FT. The key challenge in implementing AML-CFT regimes is obtaining, maintaining and disseminating relevant information. Countries should therefore treat information with: (1) the appropriate level of confidentiality and (2) reasonable level of privacy by all parties as information is a prerequisite for the effective enforcement of laws and regulations. A fundamental challenge to disseminating relevant information is establishing a framework for the sharing of information that is acceptable to all parties and meets reasonable AML-CFT objectives.

Regarding cross-border movement of funds, it has become intensely global both in volume and speed, and levels of economic crimes have also become higher and higher. There are a number of problems that law enforcement authorities face at the domestic level and are exacerbated once the crime or the proceeds cross the borders because of the differences in legal and regulatory systems. One challenging problem is related to documents held in foreign countries. When the cross-border movement of funds is made up of multi-layers of corporate entities connected to each other through a complex web of affiliates and subsidiaries, the records are spread worldwide and it is really hard to trace the fragmented movement of the funds. It can be the most challenging problem in performing asset-tracing investigation if one or two safe-haven countries are in the complex web of jurisdictions.

It is important to enact legislation that creates an environment that minimizes opportunities for unscrupulous persons to obscure the extent and nature of their participation in legal business activities. There should be effective arrangements in place that allow for the identification of all persons who participate in the ownership of corporate entities, who serve as directors or who are in positions to exert significant control over corporate vehicles.

As support at the highest level of a country is very important, policy makers will need to be convinced of the level of priority that should be accorded to the development of an AML-CFT infrastructure. An effective and efficient AML-CFT regime depends on timely legislation and members of parliament should understand the obligations that arise from the relevant UN conventions, resolutions of the Security Council and other relevant regional commitments. Enacting the bill as early as possible can be one of the challenging factors in developing a successful AML-CFT regime.

The chances of successfully implementing a regulatory regime are enhanced under circumstances in which the key stakeholders – policy makers, consumers of financial products and services, financial institutions, regulators, investigatory authorities and other government agencies – understand the competing interests and the various issues on which the regulators must focus. The challenge of understanding these factors is increased in the case of regulatory regime geared to address AML-CFT risks.

Government officials need to understand the fundamental requirements and protocols associated with their new responsibilities and the role of the FIU of the country especially in the arrangements for the handling and processing of information as it flows from reporting institutions through the FIU to law enforcement and prosecution authorities. At the same time, reporting institutions need to play their important roles as the gatekeepers of the system and to be aware of the sanctions that can arise in instances of failure to meet their legal obligations.

The establishment of a customer profile is a crucial aspect of the CDD process which is the foundation for the subsequent function of monitoring customer activity and making determination as to the need to file a suspicious activity report. It is important to update and accurately maintain information on customers, i.e. not only the information originally obtained but also all subsequent information obtained. This is a kind of on-going monitoring of customer activity and it is a challenging process. Therefore, financial institutions are challenged to determine what types of monitoring systems are most appropriate for their needs. Factors that will influence their decision are the volume, nature and complexity of their regular business transactions.

Supervisors should create and maintain an environment in which institutions are able to effectively conduct legitimate business activities with the least unnecessary regulatory burden. As they should also protect the integrity of the financial and wider business community they are challenged to develop a supervisory framework that is meaningful and effective in the context of the institutions. Regulations and guidance notes should be used to give more detailed expression to the basic framework as established in the primary legislation. Since risk-based approach that is not new to both supervisors and reporting institutions has been the center of attention, supervisors are expected to understand the risks to which their licenses are exposed and to make appropriate decisions on the most effective use of their supervisory resources.

In summary, as mentioned above, the following essential components of an effective legal framework, such as competent authorities, countermeasures against ML and FT, effective implementation, investigation of ML-FT offenses, suspicious transaction reports, good control of proceeds of crime, knowledge of untraceable ML-FT methods, international cooperation, assistance and cooperation from financial institutions and non-financial institutions, and technical assistance are important factors in the performance of combating ML-FT within an efficient and effective AML-CFT

framework. The following chapter will indicate how Thailand's AML-CFT system fulfils the requirements of such an effective regime.

It may be mentioned that specific details about the need for compliance with international standards and the need for improvement of Thailand's AML laws by amendment, new enactment, and modification of existing regulations, guidelines, etc. can be seen in the concluding Chapter X.