Guidance Notes on AML&CFT for Insurance Companies

Anti Money Laundering Department

Bangladesh Bank

Focus Group

Md. Eskandar Miah, Deputy General Manager Anti Money Laundering Department, Bangladesh Bank	**Convener**
Md. Mizanur Rahman, Deputy Controller Insurance Development and Regulatory Authority	**Member**
S.M. Ibrahim Hossain, Faculty Member Bangladesh Insurance Academy	**Member**
Mohammad Abdus Salam, Assistant General Manager Sadharan Bima Corporation	**Member**
Md. Masud Miah, Manager Accounts Jiban Bima Corporation	**Member**
Mollah Md. Nurul Islam, Secretary General Bangladesh Insurance Association	**Member**
M. Ala Uddin Ahmad, Financial Controller Metlife Alico	**Member**
Md. Sabir Ahmed, Head of Finance Reliance Insurance Ltd	**Member**
Md. Rafiq Ahmed, Jt Senior Vice President Prime Islami Life Insurance Ltd	**Member**
Bashir Ahmed, Assistant General Manager Sonar Bangla Insurance Ltd	**Member**
Md. Altaf Hossain, Deputy General Manager Nitol Insurance Company Ltd	**Member**
Mohammed Nur Hossain, Deputy Manager Sunflower Life Insurance Co. Ltd	**Member**
Kamal Hossain, Deputy Director Anti Money Laundering Department, Bangladesh Bank	**Member Secretary**

Review Team

Naba Gopal Banik
Member, Insurance Development and Regulatory Authority

Abu Hena Mohammad Razee Hassan
Executive Director, Bangladesh Bank

Md. Rezaul Karim
Managing Director, Sadharan Bima Corporation

Parikshit Datta Choudhury
Managing Director, Jiban Bima Corporation

Akthar Ahmed
Managing Director, Reliance Insurance Ltd

P. K. Roy
Managing Director, Rupali Insurance Company Ltd

Noor Mohammad Bhuiyan
Managing Director, Rupali Life Insurance Co. Ltd

Preface

The methods and techniques of Money Laundering (ML) and Terrorist Financing (TF) are ever evolving process and changing in response to developing counter measures. For that reason, Financial Action Task Force (FATF), the international standard setter on anti money laundering (AML) and combating terrorist financing (CFT), has revised its 40 (forty) recommendations for AML and 9 (nine) special recommendations for CFT.

In line with the international standards and initiatives, Bangladesh has also amended its Money Laundering Prevention Act (MLPA), 2002 and enacted MLPA, 2009. To combat Terrorism and Terrorist Financing Anti Terrorism Act (ATA), 2009 has also been enacted. Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML&TF through issuing instructions and directives for reporting agencies including Insurance Companies (ICs).

To perform the responsibilities and exercises the power laid down in the acts by BB, this guidance notes titled "Guidance Notes on Anti Money Laundering & Combating Financing of Terrorism" is prepared for ICs functioning in Bangladesh. This Guidance Note is deemed to be the national best practice but not constitute a legal interpretation of the said acts but it is designed to assist ICs to comply with the Bangladesh's AML & CFT regulation.

As per this Guidance Notes, ICs are advised to formulate their own guidance notes approved by their Board of Directors (BoD). It is recognized that ICs may have systems and procedures in place which, while not identical to those outlined in these Guidance Notes, nevertheless impose controls and procedures which are at least equal to, if not higher than, those contained in these Guidance Notes. Because of the vulnerabilities of insurance sector being used by money launderers and terrorist financiers, BB, as part of its supervisory process, will assess the adequacy of the AML & CFT program including internal controls, policies and procedures and the degree of compliance of the ICs.

An overriding aim of the Money Laundering Regulations and the Guidance Notes is to ensure that appropriate identification information is obtained in relation to the policy holders of ICs and the payments made to them. Furthermore, this is to assist the detection of suspicious transactions and/or activities and also to create an effective "audit trail" in the event of an investigation, subsequently. ICs are specially advised to be focused and give more emphasis on identification and reporting of suspicious transactions and/or activities.

It is expected that all ICs conducting their own business pay due regard to the Guidance Notes in developing responsible anti-money laundering procedures suitable to their situation. If an IC appears not to be doing so, then BB may seek an explanation or may conclude that the IC is carrying on business in a manner that may give rise to sanctions under the applicable legislation.

It is important that the management of ICs should view prevention of ML&TF as part of their risk management strategies, not simply as a stand-alone requirement that is being imposed by the legislation. Thus the management may achieve confidence that their organizations are not being abused by the money laundered or terrorist financers.

Table of Contents

List of Abbreviations

ACC	Anti Corruption Commission
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
AMLD	Anti-Money Laundering Department of Bangladesh Bank
APG	Asia Pacific Group on Money Laundering
ATA	Anti Terrorism Act
ATO	Anti Terrorism Ordinance
BB	Bangladesh Bank
BDT	Bangladesh Taka
CAMLCO	Chief Anti-Money Laundering Compliance Officer
CDD	Customer Due Diligence
CTC	Counter Terrorism Committee
CTR	Cash Transaction Report
DEA	Drug Enforcement Agency
EDD	Enhanced Due Diligence
FATF	Financial Actions Task Force
FCBs	Foreign Commercial Banks
FIU	Financial Intelligence Unit
FSRB	FATF Style Regional Body
GoB	Government of Bangladesh
IAIS	International Association of Insurance Supervisors
ICs	Insurance Companies
ICRG	International Cooperation and Review Group
IOSCO	International Organization of Securities Commissioners
KYC	Know Your Customer
MER	Mutual Evaluation Report
ML	Money Laundering
MLPA	Money Laundering Prevention Act

MLPO	Money Laundering Prevention Ordinance
NCC	National Coordination Committee on AML/CFT
NCCT	Non-cooperating Countries and Territories
PEPs	Politically Exposed Persons
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
TF	Terrorist Financing
TP	Transaction Profile
UNCAC	United Nations Convention Against Corruption
UNODC	UN Office of Drugs and Crime
UNSCR	United Nations Security Council Resolution

Chapter 1: Basics of Money Laundering and Terrorist Financing

1.1 Introduction

For most countries, money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques used to launder money and finance terrorism add to the complexity of these issues. Such sophisticated techniques may involve: multiple financial transactions, the use of different financial instruments and other kinds of value-storing assets; different types of financial institutions, accountants, financial advisers, shell corporations and other service providers; complex web of transfers to, through, and from different countries.

A less simple concept, however, is defining terrorism itself, because the term may have significant political, religious, and national implications from country to country. Money laundering and terrorist financing often display similar transactional features, mostly having to do with concealment and disguise.

Money launderers send illicit funds through legal channels in order to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use. But the result is the same—reward. When money is laundered, criminals profit from their actions; they are rewarded by concealing the criminal act that generates the illicit proceeds and by disguising the origins of what appears to be legitimate proceeds. Similarly, those who finance terrorism are rewarded by concealing the origins of their funding and disguising the financial support to carry out their terrorist stratagems and attacks.

1.2 What is Money Laundering?

Money laundering can be defined in a number of ways. But the fundamental concept of Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;

- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

The Financial Action Task Force on Money Laundering (FATF)[1], which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term "money laundering" succinctly as "the processing of…criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gains of crime.

Money Laundering is defined in Section 2 (3) of the Prevention of Money Laundering Act 2009 as follows:

Money Laundering means:

i) transfer, conversion, bringing/ remitting funds in and out of Bangladesh the proceeds or properties acquired through commission of a predicate offence[2] for the purpose of concealing or disguising the illicit origin of the property or illegal transfer of properties acquired or earned through legal or illegal means.

ii) to conduct, or attempt to conduct a financial transaction with an intent to avoid a reporting requirement under this Act (the MLPA, 2009).

iii) to do or attempt to do such activities so that the illegitimate source of the fund or property can be concealed or disguised or knowingly assist to perform or conspire to perform such activities.

1.3 What Is Terrorist Financing

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

1. If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

   a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or

   b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

2....

[1] Please see section 4.3 for explanation

[2] Predicate offence is the underlying criminal activity that generated proceeds, which when laundered, results in the offense of money laundering.

3. For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

Some countries face difficulties in defining terrorism as not all countries have adopted the conventions agreed on specifically what actions constitute terrorism. In addition, the meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country. FATF, which is recognized as the international standard setter for combating financing of terrorism (CFT) efforts, does not specifically define the term financing of terrorism in its nine Special Recommendations on Terrorist Financing (Special Recommendations). Nonetheless, FATF urges countries to ratify and implement the 1999 United Nations International Convention for Suppression of the Financing of Terrorism. Thus, the above definition is the one most countries have adopted for purposes of defining terrorist financing.

According to the article 7 of the Anti Terrorism Act, 2009 of Bangladesh, **financing of terrorism** means:

(1) Whoever provides or incites to provide money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(2) Whoever receives money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(3) Whoever arranges money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(4) A person guilty of the offence as described in the subsections from 1 to 3 shall be punished with imprisonment for a term which may extend to twenty years and it shall not be less than three years, to which fine may also be added.

1.4 The Link between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

For these reasons, FATF has recommended that each country criminalize the financing of terrorism, terrorist acts and terrorist organizations, and designate such offenses as money laundering predicate offenses. Finally, FATF has stated that the nine Special Recommendations combined with The Forty Recommendations on money laundering

constitute the basic framework for preventing, detecting and suppressing both money laundering and terrorist financing.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations. Consequently, this difference requires special laws to deal with terrorist financing. However, to the extent that funds for financing terrorism are derived from illegal sources, such funds may already be covered by a country's AML framework, depending upon the scope of predicate offenses for money laundering.

1.5 Why Money Laundering is done

Criminals engage in money laundering for three main reasons:

First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

1.6 Laundering Techniques

Obviously there is no one way of laundering money or other property. It can range from the simple method of using it in the form in which it is acquired to highly complex schemes involving a web of international businesses and investments. In general, money laundering process comprises three stages:

Placement – placing the criminal funds into the financial system directly or indirectly.

Layering – the process of separating criminal proceeds from their source by using complex layers of financial transactions designed to hide the audit trail and provide anonymity.

Integration – if the layering process succeeds, integration schemes place the laundered proceeds back into the legitimate economy in such a way that they appear to be normal business funds.

This three stage model is more often occur simultaneously or overlap depending on the facilities of the launderer, the requirements of the criminals, and on the robustness, or otherwise, of the regulatory and legal requirements.

Chapter 2: Vulnerabilities of Insurance Companies to ML/TF

2.1 Introduction

Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (cash or bank transfer) and contract. Insurers should take these factors into account when assessing ML/TF risks and vulnerabilities. This means they should prepare a risk profile of every type of business in general and of each business relationship.

2.2 ML/TF Risks for Insurance Companies (ICs)

According to the nature of business, what ICs do is to hedge insured's risks in some way. But ICs are to face several types of risks of money laundering and terrorist financing, such as:

- Reputational risk
- Legal risk
- Operational risk (failed internal processes, people and systems & technology)
- Concentration risk (regarding customer segments or sectors)

All risks are inter-related and together have the potential of causing serious threat to the survival of the insurance companies

2.2.1 Reputational Risk

- The potential that adverse publicity regarding an IC's business practices, whether accurate or not, will cause a loss of confidence in the integrity of the institution
- Reputational Risk : a major threat to ICs as confidence of insurers, re-insurers and general market place to be maintained
- ICs are vulnerable to Reputational Risk as they can be a vehicle for or a victim of customers' illegal activities

2.2.2 Operational Risk

- The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events
- Weaknesses in implementation of ICs' programs, ineffective control procedures and failure to practice due diligence

2.2.3 Legal Risk

- The possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of an IC
- ICs may become subject to lawsuits resulting from the failure to observe compliance requirements, mandatory KYC standards or from the failure to practice due diligence

- ICs can suffer fines, criminal liabilities and special penalties imposed by supervisors according to MLPA 2009.

2.2.4 Concentration Risk

- The risk that too much business is being conducted with persons or corporations belonging to the same conglomerate, group or geographical area.
- Too much concentration in single and risky sectors
- On liabilities side: Risk of early and sudden encashment of big policy to liquidity

2.3 Instances of Vulnerabilities

2.3.1 Life insurance

The types of life insurance contracts that are vulnerable as a vehicle for money laundering or terrorist financing are products, such as:

- unit-linked or with profit single premium contracts,
- single premium life insurance policies that store cash value,
- fixed and variable annuities, and
- (Second hand) endowment policies.

When a life insurance policy matures or is surrendered or insured event occurs, policy proceeds become available to the policyholder or his/her beneficiaries. The beneficiary of the policy may be changed in order that payments are made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.

> Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

2.3.2 Non-life insurance

Non-life insurance money laundering or terrorist financing can be seen through inflated or totally bogus claims, e.g. by arson or other means causing a bogus claim to be made to recover part of the invested illegitimate funds. Other examples include cancellation of policies for the return of premium by an insurer's cheque, and the overpayment of premiums with a request for a refund of the amount overpaid. Money laundering can also occur through under-insurance, where a criminal can say that he received compensation for the full amount of the damage, when in fact he did not. Specific cases of money laundering are-

> Four broking agencies were forced to freeze funds after US court action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, codenamed Golden Jet, was coordinated by the Drug Enforcement Agency (DEA) based in the USA but also involved the FBI and the UK authorities. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft.

2.3.3 Intermediaries

Insurance intermediaries − independent or otherwise − are important for distribution, underwriting and claims settlement. They are often the direct link to the policyholder and therefore intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The FATF Recommendations allow insurers, under strict conditions, to rely on customer due diligence carried out by intermediaries. The same principles that apply to insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of, or does not conform to, necessary procedures, or who fails to recognise or report information regarding possible cases of money laundering or the financing of terrorism. The intermediaries themselves could have been set up to channel illegitimate funds to insurers. In addition to the responsibility of intermediaries, customer due diligence ultimately remains the responsibility of the insurer involved. Specific cases of money laundering are-

An insurance company was established by a well-established insurance management operation. One of the clients, a previously communist country's insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment routed out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured.

2.3.4 Reinsurance

Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions. Examples include:

- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds
- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding
- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

A state insurer in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the company was linked to potential war lords and drug traffickers. A report was made to the law enforcement authorities.

2.3.5 Return premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time
- return premium being credited to an account different from the original account
- requests for return premiums in currencies different to the original premium, and
- regular purchase and cancellation of policies.

2.3.6 Over payment of premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums, has, been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say BDT 50,000 or equivalent)
- the request to refund the excess premium was to a third party
- the assured is in a jurisdiction associated with money laundering and
- where the size or regularity of overpayments is suspicious.

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

2.3.7 Claims

A claim is one of the principal methods of laundering money through insurance. Outlined below are examples of where claims have resulted in reports of suspected money laundering and terrorist financing.

> A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the client's creditors discovering funds that had allegedly been smuggled overseas. Documents indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering.
>
> A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest "dirt money" for a profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organized by the purchasers to ensure a claim occurred

and that they received “clean” money as a claims settlement.

Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

2.3.8 Assignment of claims

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travelers' cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

Cases of vulnerabilities are stated in Annexure A

Chapter 3: Impacts of ML/TF on Developing Countries

3.1 Introduction

Criminals and terrorist succeed largely in concealing the origins or sources of their funds and sanitize the proceeds by moving them through national and international financial systems. While money laundering and the financing of terrorism can occur in any country, they have particularly significant economic and social consequences for developing countries like Bangladesh. The absence of, or a lax in AML/CFT regime in a particular country permits criminals and those who finance terrorism to operate, using their financial gains to expand their criminal pursuits and fostering illegal activities such as corruption, drug trafficking, illicit trafficking and exploitation of human beings, arms trafficking, smuggling, and terrorism. But the magnitude of such adverse impacts cannot be quantified with precision.

3.2 The Adverse Implications for Developing Countries

3.2.1 Increased Crime and Corruption

If money laundering is prevalent in a country, it generates more crime and corruption in critical gateways. To the extent that a country is viewed as a safe haven for money laundering, it is likely to attract criminals and promote corruption. Safe haven includes-

- weak AML/CFT framework,
- little enforcement of AML/CFT provisions,
- limited number of predicate offences,
- limited inclusion of reporting institutions,
- ineffective penalties etc.

A comprehensive and effective AML/CFT framework, together with timely implementation and effective enforcement, on the other hand, significantly reduce the profitable aspects of criminal activities and, in fact, discourage criminals and terrorists from utilizing a country. This is especially true when the proceeds from criminal activities are aggressively confiscated and forfeited as part of a country's overall AML/CFT legal framework.

3.2.2 Hassle from Foreign Counterparts

Foreign financial institutions may decide to limit their transactions with institutions from money laundering havens, subject these transactions to extra scrutiny making them more expensive, or terminate correspondent or lending relationships altogether. Even legitimate businesses and enterprises from money laundering havens may suffer from reduced access to world markets or access at a higher cost due to extra scrutiny of their ownership, organization and control systems.

Any country known for lax enforcement of AML/CFT is less likely to receive foreign private investment. For developing nations, eligibility for foreign governmental assistance is also likely to be severely limited.

Foreign direct investment and foreign aid may be reduced or withdrawn because of lax enforcement of AML/CFT measures.

Finally, the Financial Action Task Force on Money Laundering (FATF) maintains a list of countries that do not comply with AML requirements or that do not cooperate sufficiently in the fight against money laundering i.e. "non-cooperating countries and territories" (NCCT) list, gives public notice that the listed country does not have in place even minimum standards. Beyond the negative impacts referred to here, individual FATF member countries could also impose specific counter-measures against a country that does not take action to remedy its AML/CFT deficiencies.

3.2.3 Weakened Financial Sector

Money laundering and terrorist financing can loose the knitting of a country's financial sector, as well as the stability of individual financial institutions in multiple ways. The adverse consequences may arise from reputational, operational, legal and concentration risks. Each has specific costs, say for insurance companies:

- Loss of profitable business
- Liquidity problems through pre mature encashment
- Termination of re-insurance banking facilities
- Investigation costs and fines
- Asset seizures
- Loan losses and
- Declines in the stock value of ICs

3.2.4 Compromised Economy and Private Sector

Money launderers may use front companies[3] to co-mingle the illicit funds with legitimate funds in order to hide the ill-gotten proceeds, not to earn profit. Access to illicit funds let front companies to subsidize the front company's products and services, even at below-market prices. As a consequence, legitimate enterprises find it difficult to compete with such front companies. Thus by using front companies and other investments in legitimate companies money laundering proceeds can be utilized to control whole industry or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

3.2.5. Damaged Privatization Efforts

Money launderers threaten the efforts of many countries to reform their economies through privatization. These criminal organizations are capable of outbidding legitimate purchasers of former state-owned enterprises. When illicit proceeds are invested in this manner, criminals increase their potential for more criminal activities and corruption, as well as deprive the country of what should be legitimate, market-based, taxpaying enterprise.

[3] Business enterprises that appear legitimate and engage in legitimate business but are, in fact, controlled by criminals

3.3 The Benefits of an Effective AML/CFT Framework

A strong AML/CFT institutional framework that includes a broad scope of predicate offenses for money laundering helps to fight crime and corruption. An effective AML/CFT regime is deterrent to criminal activities. In this regard, confiscation and forfeiture of money laundering proceeds eliminates profits from criminal activities, thereby reducing the incentive to commit criminal acts.

In addition, an effective AML/CFT regime reduces the potential that institutions can experience losses from fraud. Proper customer identification procedures and determination of beneficial ownership provide specific due diligence for higher risk policies and permit monitoring for suspicious activities. Such prudential internal controls are consistent with the safe and sound operation of a financial institution. Public confidence on financial institutions is enhanced.

Strong AML/CFT regimes provide a disincentive for the criminal involvement in the economy. This permits investments to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

Chapter 4: International Initiatives & standards

4.1 Introduction

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. This part of this Guidance Notes discusses the various international organizations that are viewed as the international standard setters. It further describes the documents and instrumentalities that have been developed for anti-money laundering (AML) and combating the financing of terrorism (CFT) purposes.

4.2 The United Nations

The United Nations (UN) was the first international organization to undertake significant action to fight money laundering on a truly world-wide basis. The UN is important in this regard for several reasons.

First, it is the international organization with the broadest range of membership. Founded in October of 1945, there are currently 191 member states of the UN from throughout the world.

Second, the UN actively operates a program to fight money laundering; the Global Program against Money Laundering, which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).

Third, and perhaps most importantly, the UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws.

In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other action on the part of an individual country.

4.2.1 The Vienna Convention

Due to growing concern about increased international drug trafficking and the tremendous amounts of related money entering into banking system, the UN, adopted the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as Vienna Convention, named after the city in which it was signed. The Vienna Convention deals primarily with provisions to fight the illicit drug trade and related law enforcement issues. At present, nearly 169 countries including Bangladesh are party to the convention. The convention came into force on November 11, 1990.

4.2.2 The Palermo Convention

In order to fight against internationally organized crimes, the UN adopted The International Convention against Transnational Organized Crime (2000), named after the city in which it was signed as Palermo Convention. The Palermo Convention specifically obligates each ratifying country to:

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;
- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
- Promote international cooperation.

This convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries.

4.2.3 International Convention for the Suppression of the Financing of Terrorism

The financing of terrorism was an international concern prior to the attacks on the United States on September 11, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries ratifying it.

The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds with the (1) intent that the funds be used for, or (2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

4.2.4 Security Council Resolution 1373

Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

- deny all forms of support for terrorist groups;

- suppress the provision of safe haven or support for terrorist, including freeing funds or assets of persons, organizations or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorists; and
- cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

4.2.5 Security Council Resolution 1267 and Successors

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the "Sanctions Committee" (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999, dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002), and measures to improve implementation (1455 of January 17, 2003).

The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.

4.2.6 Global Program against Money Laundering

The UN Global Program against Money Laundering (GPML) is within the UN Office of Drugs and Crime (UNODC). The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request.

4.2.7 The Counter-Terrorism Committee

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism.

Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.

4.3 The Financial Action Task Force

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 33 countries and territories and two regional organizations.

FATF performs three primary functions with regard to money laundering:

1) monitoring members' progress in implementing anti-money laundering measures;
2) reviewing and reporting on laundering trends, techniques and countermeasures; and
3) promoting the adoption and implementation of FATF anti-money laundering standards globally.

4.3.1 The Forty Recommendations for ML

FATF has adopted a set of 40 recommendations, The Forty Recommendations on Money Laundering (The Forty Recommendations), which constitute a comprehensive framework for AML and are designed for universal application by countries throughout the world. Although not binding as law upon a country, The Forty Recommendations have been widely endorsed by the international community and relevant organizations as the international standard for AML.

The Forty Recommendations were initially issued in 1990 and revised in 1996 and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally.

4.3.2 The Nine Special Recommendations for TF

FATF also focuses its expertise on the world-wide effort to combat terrorist financing. To accomplish this expanded mission FATF has adopted nine Special Recommendations on Terrorist Financing (Special Recommendations). As part of this effort, FATF members use a self-assessment questionnaire of their country's actions to come into compliance with the Special Recommendations. FATF is continuing to develop guidance on techniques and mechanisms used in the financing of terrorism.

4.3.3 Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of The Forty Recommendations is facilitated by a two-stage process: self assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of The Forty Recommendations. In the

mutual evaluation stage, each member is examined and assessed by experts from other member countries.

4.3.4 Reporting on Money Laundering Trends and Techniques

One of FATF's functions is to review and report on money laundering trends, techniques and methods (also referred to as typologies). To accomplish this aspect of its mission, FATF issues annual reports on developments in money laundering through its Typologies Report. These reports are very useful for all countries, not just FATF members, to keep current with new techniques or trends to launder money and for other developments in this area.

4.3.5 The NCCT List

One of FATF's objectives is to promote the adoption of international AML/CFT standards for all countries. Thus, its mission extends beyond its own membership, although FATF can only sanction its member countries and territories. Thus, in order to encourage all countries to adopt measures to prevent, detect and prosecute money launderers, i.e., to implement the Forty Recommendations, FATF has adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in this area. The process uses 25 criteria, which are consistent with The Forty Recommendations, to identify such non-cooperative countries and territories (NCCT's) and place them on a publicly available list.

An NCCT country is encouraged to make rapid progress in remedying its deficiencies. In the event an NCCT country does not make sufficient progress, counter-measures may be imposed. Counter measures consist of specific actions by FATF member countries taken against an NCCT-listed country.

In addition to the application of applying special attention to business relationships and transactions from such countries, FATF can also impose further counter-measures, which are to be applied in a gradual, proportionate and flexible manner; these include:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;
- In considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of banks, taking into account the fact that the relevant bank is from an NCCT;
- Warning non-financial sector businesses that transactions with entities within the NCCTs might run the risk of money laundering.

Finally, these counter measures may include FATF-member countries terminating transactions with financial institutions from such a country.

Most countries make a concerted effort to be taken off the NCCT list because it causes significant problems for their financial institutions and businesses with respect to international transactions, as well as their reputation internationally.

4.3.6 ICRG

The FATF has set up the International Co-operation Review Group (ICRG) as a new process that is designed to notably engage the 'unwilling' and those jurisdictions that pose a real risk to the international financial system. The ICRG process is designed to bind FATF and FSRB members that show effective commitment to the standards against those that evade their international obligations. The time and money that one jurisdiction spend on creating an effective AML/CFT system in that country is wasted if neighbor remains a safe haven for criminals. The ICRG process is focused on specific threats and specific risk in specific countries. If need be these jurisdictions may be publicly identified by the FATF Plenary.

The second role of the ICRG is to work with those jurisdictions to remedy the shortcomings underpinning the judgment of the FATF Plenary. That means that there could be a focused follow up process between the ICRG and a specific jurisdiction. If all evaluation reviews and regular follow ups are conducted properly, there should be no duplication or conflict within the FATF family and between the follow up processes.

4.3.7 Methodology for AML/CFT Assessments

In 2002, the FATF, International Monetary Fund (IMF), and World Bank adopted a single assessment methodology to be used both by FATF in its mutual evaluations and by the IMF and World Bank in their assessments under their financial sector assessment and offshore financial center programs. The FATF-style regional bodies (FSRBs) subsequently agreed to use it for their mutual evaluations.

The methodology was revised in 2004, following the 2003 revision of The Forty Recommendations. The methodology set out over 200 'essential criteria' that assessors should examine when carrying out assessments of an AML and CFT regime.

4.4 The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of 10 countries. Individual countries are represented by their central banks, or by the relevant authorities with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank supervisory issues. These standards and guidelines are adopted with the expectation that the appropriate authorities within each country will take all necessary steps to implement them through detailed measures, statutory, regulatory or otherwise, that best

suit that country's national system. Three of the Basel Committee's supervisory standards and guidelines concern money laundering issues.

4.4.1 Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic policies and procedures that bank managements should undertake to assist in suppressing money laundering. There are essentially four principles contained in the Statement on Prevention:

- Proper customer identification;
- High ethical standards and compliance with laws;
- Cooperation with law enforcement authorities; and
- Policies and procedures to adhere to the statement.

4.4.2 Basel Core Principles for Banking

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provides a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. Of the total 25 Core Principles, one of them, Core Principle 15, deals with money laundering; it provides:

> Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know your customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.

These "know your customer" or "KYC" policies and procedures are a crucial part of an effective AML/CFT institutional framework for every country.

In addition, the Basel Committee issued a "Core Principles Methodology" in 1999, which contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures. These, additional criteria include specific reference to compliance with The Forty Recommendations.

4.4.3 Customer Due Diligence

In October, 2001, the Basel Committee issued an extensive paper on KYC principles entitled, Customer due diligence for banks (Customer Due Diligence). This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards build upon and provide more specific information on the Statement on Prevention and Core Principle 15.

4.5 International Association of Insurance Supervisors

The International Association of Insurance Supervisors (IAIS), established in 1994, is an organization of insurance supervisors from more than 100 different countries and jurisdictions.

Its primary objectives are to:

- Promote cooperation among insurance regulators,
- Set international standards for insurance supervision,
- Provide training to members, and
- Coordinate work with regulators in the other financial sectors and international financial institutions.

In addition to member regulators, the IAIS has more than 60 observer members, representing industry associations, professional associations, insurance and reinsurance companies, consultants and international financial institutions.

While the IAIS covers a wide range of topics including virtually all areas of insurance supervision, it specifically deals with money laundering in one of its papers. In January 2002, the association issued Guidance Paper No. 5, Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities (AML Guidance Notes). It is a comprehensive discussion on money laundering in the context of the insurance industry. Like other international documents of its type, the AML Guidance Notes are intended to be implemented by individual countries taking into account the particular insurance companies involved, the products offered within the country, and the country's own financial system, economy, constitution and legal system.

The AML Guidance Notes contain four principles for insurance entities:

- Comply with anti-money laundering laws,
- Have "know your customer" procedures,
- Cooperate with all law enforcement authorities, and
- Have internal AML policies, procedures and training programs for employees.

These four principles parallel the four principles in the Basel Committee's Statement on Prevention. The AML Guidance Notes are entirely consistent with The Forty Recommendations, including suspicious activity reporting and other requirements. In fact, The Forty Recommendations are included in an appendix to the IAIS's AML Guidance Notes.

4.6 International Organization of Securities Commissioners

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 105 countries. With regard to money laundering, IOSCO passed a "Resolution on Money Laundering" in

1992. Like other international organizations of this type, IOSCO does not have law-making authority. Similar to the Basel Committee and IAIS, it relies on its members to implement its recommendations within their respective countries

4.7 The Egmont Group of Financial Intelligence Units

In 1995, a number of governmental units known today as Financial Intelligence Units (FIUs) began working together and formed the Egmont Group of FIUs (Egmont Group), named after the location of its first meeting at the Egmont-Arenberg Palace in Brussels. The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

The mission of the Egmont Group was expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country's FIU must first meet the Egmont FIU definition, which is "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 and potential financing of terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing." Bangladesh FIU applied for membership in the Egmont Group.

4.8 Asia Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 40 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations and Nine Special Recommendations on Terrorist Financing of the Financial Action Task Force on Money Laundering (FATF).

The APG has five key roles:

- To assess compliance by APG members with the global AML/CFT standards through a robust mutual evaluation program;

- To coordinate bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region in order to improve compliance by APG members with the global AML/CFT standards;
- To participate in, and co-operate with, the international anti-money laundering network - primarily with the FATF and with other regional anti-money laundering groups;
- To conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- To contribute to the global policy development of anti-money laundering and counter terrorism financing standards by active Associate Membership status in the FATF.

The APG also assists its members to establish coordinated domestic systems for reporting and investigating suspicious transaction reports and to develop effective capacities to investigate and prosecute money laundering and the financing of terrorism offences.

Chapter 5: National Initiatives

Considering money laundering/ Terrorist Financing as national problems Bangladesh has taken the following initiatives:

- Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards on AML/CFT in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40+9 recommendations. Subsequently, Bangladesh promulgated Money Laundering Prevention Act (MLPA), 2002 which came into force on 30 April, 2002.

- After 9/11 terrorist attack in USA, AML/CFT initiatives got momentum all over the world. In the process of responding to international concern, Bangladesh Government formed a central and regional taskforce on 27 January, 2002 to combat money laundering and illegal Hundi activities in Bangladesh.

- Bangladesh was the first among the South Asian countries to enact MLPA. To implement MLPA, Bangladesh Bank established a separate department named Anti Money Laundering Department (AMLD) in July, 2002.

- The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and adopted by the APG in September, 2003. The 2002-03 assessment was undertaken prior to the revisions of the FATF 40 Recommendations and the FATF Assessment methodology, 2002 was applied. The first ME took place just after the enactment of the MLPA, 2002, which came into force on 30 April 2002.

- Bangladesh Bank (BB) issued Guidance Notes titled 'Guidance Notes on prevention of Money Laundering' in 2003 for Banks to let them effectively understand and formulate separate guidance notes for themselves. Formulation of Guidance Notes for other reporting agencies is under process.

- On May 16, 2007 financial intelligence unit (FIU) was established in BB for receiving, analyzing and disseminating suspicious transaction reports (STR) related to ML/TF and cash transaction report (CTR) received by AMLD, BB.

- Self assessment and independent testing procedure system were introduced for banks on March 24, 2008 to assess their own AML/CFT compliance. Side by side, Bangladesh Bank has also been monitoring the same through the process called system check inspection.

- A rigorous Customer Due Diligence (CDD) procedure has been introduced to protect identity theft by customer through issuance of Uniform Account Opening form for all

banks. It includes standardized KYC, Transaction Profile (TP), risk grading of customers.

- MLPA empowers the FIU to enter into agreements and arrangements with foreign FIUs to receive and request information in relation to money laundering offences or suspicious transactions. To facilitate exchange of information and intelligence among FIUs Bangladesh FIU has already signed 10 (ten) MoUs with other FIUs and several other MoUs signing procedure are under process.
- To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009.
- To combat terrorism and terrorist financing Bangladesh also enacted Anti Terrorism Act (ATA), 2009. The ATA tightens the terrorist financing regime in Bangladesh. The ATA authorizes the filing of suspicious transaction reports (STRs) related to TF, empowers the central bank to monitor suspected financial transactions related to TF and thus prohibits a person from possessing property or proceeds of terrorist activity. In accordance with the ATA, property or proceeds of terrorist activities are liable to be confiscated and forfeited to the government.
- The 2nd round AML/CFT Mutual Evaluation of Bangladesh was conducted in August, 2008. The report was adopted by the APG Plenary in July, 2009. The Mutual Evaluation Report (MER) presents a comprehensive assessment of the progress and deficiencies of Bangladesh AML/CFT regime and identifies the areas for further improvement.
- Bangladesh Government is highly committed to combat ML and TF thus importance has been attached to the MER recommendations and has given utmost effort to implement those recommendations. To implement recommendations of 2nd MER Bangladesh Government along with respective organizations has taken the following initiatives:
    - Constituted National Coordination Committee on AML/CFT headed by the Hon'ble Finance Minister
    - Constituted Working Committee that consists of all regulatory authorities headed by secretary of Finance Ministry.
    - Conducted in-country Strategic Implementation Planning (SIP).
    - Issued a comprehensive circular for banks, non bank financial institutions, money changers and money remitters. The circular addressed the following issues
        - the CDD process including EDD
        - PEPs related issue

- Beneficial ownership
- Shell Banks
- Correspondent Banking relationship
- Employee screening mechanism
- Training and awareness etc.

- Amendment of MLPA and ATA
- Accession to Palermo Convention
- Inclusion of ML and TF offences in Extradition act, 1974 and
- Enactment of Mutual Legal Assistance Act etc.

- Bangladesh Government has formulated the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2011-2013 as part of its action plan. The strategy consists of 12 (twelve) strategies:

1. Strengthening the AML/CFT legal framework
2. Enhancing effectiveness of the FIU
3. Enforcing compliance of all reporting agencies
4. Structural improvement and capacity building in tracing out methods, techniques and channels of money laundering and terrorist financing
5. Improving transparency in financial reporting on AML/CFT issues
6. Ensuring transparency in the ownership of legal entities
7. Enhancing financial inclusion
8. Maintaining a comprehensive AML/CFT database
9. Boosting national coordination both at policy and operational levels
10. Developing and maintaining international and regional cooperation on AML/CFT
11. Heightening public awareness
12. Stemming the illicit outflows and inflows of fund

Chapter 6: Anti Money Laundering Compliance Program

6.1 Introduction

Insurance Companies (ICs) are subject to AML/CFT laws and should establish and maintain an effective AML/CFT program that includes at least the following:

- Development of internal policies, procedures and controls;
- Appointment of an AML/CFT compliance Officer;
- Ongoing employee training; and
- Independent audit function including internal and external audit function to test the effectiveness and efficiency of the program.

The compliance program should be documented, approved by the Board of Directors and communicated to all levels of the organization. In developing an AML/CFT compliance program, attention should be paid to the size and range of activities, complexity of operations, and the nature and degree of ML/FT risks facing an institution. ICs can follow risk based approach for AML/CFT.

6.2 Statutory and International Requirements

FATF (the international standard setter) recommendation 15 requires that financial institutions have an internal control program.

Section 25 of the Money Laundering Prevention Act, 2009 requires reporting organizations that include ICs and section 15 of the Anti Terrorism ACT, 2009 requires ICs to comply with the following to combat money laundering and terrorist financing.

6.3 Internal Policies, Procedures and Controls

6.3.1 Policies

AML/CFT policy usually includes the following key elements

- High level summary of key controls, Objectives of the policy (e.g. to protect the reputation of the institution);
- Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the business, including on a global basis);
- Waivers and exceptions;
- Operational controls;

Key operational controls of an AML/CFT policy

The following elements should be included in the operational controls of an AML/CFT policy:

- Statement of responsibility for compliance with AML/CFT policy;
- Customer due diligence:
  - Customer identification/ verification
  - Additional know your customer information

- High risk customers
- Non face to face business (if applicable)
- Reinsurance arrangements
- Handling of politically exposed persons

- Monitoring of suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping ;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach.

The Role of Senior Management must be elaborated in the policy

The most important element of a successful AML/CFT program is the commitment of senior management, including the Managing Director/ Chief Executive Officer, and the board of directors, to the development of AML/CFT objectives and the implementation of AML/CFT measures which can deter criminals from using their institutions for ML/TF.

Senior management must send the signal that the corporate is concerned as about its reputation as about profits, marketing, and customer service. As part of its anti- money laundering policy, all ICs should communicate clearly with all of their employees on an annual basis in a statement from the chief executive officer that vividly sets forth its policy against ML/TF and any activity which facilitates ML/TF. Such a statement should evidence the strong commitment of the institution and its senior management to comply with all laws and regulations designed to combat ML/TF.

The statement of compliance policy should at a minimum include:

- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
- A statement that all activities carried on by the ICs must comply with applicable governing laws and regulations.
- A statement that complying with rules and regulations is the responsibility of each individual in the ICs in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for non-compliance.
- The statement should direct staff(s) to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- A statement that employees will be held accountable for carrying out their compliance responsibilities.

Written Anti-Money Laundering Compliance Policy

The board of directors of each IC must develop, administer, and maintain an anti money laundering compliance policy that ensures and monitors compliance with the Act, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

The written anti money laundering compliance policy, at a minimum, should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the law.

The Policies should be based on an assessment of ML/TF risks, taking into account the ICs' business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to ML/TF.

It should include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures should address its KYC policy and identification procedures before establishing customer relationship, monitoring existing policies for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

It should-

- Include a description of the roles of the Anti-Money Laundering Compliance Officers(s)/Unit and other appropriate personnel.
- Develop and implement screening programs to ensure high standards when hiring employees. Implement standards for employees who consistently fail to perform in accordance with the AML/CFT framework.
- Incorporate money laundering compliance into job descriptions and performance evaluations of appropriate personnel.
- Have the arrangements for program continuity despite changes in management or employee composition or structure.

The AML/CFT policies should be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing anti money laundering rules and regulations or businesses.

In addition, the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and set forth the consequence of noncompliance with the applicable laws and the institution's policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with ML/TF.

6.3.2 Procedures

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. It will be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures and the process should be reviewed and updated regularly.

6.3.3 Controls

The program also shall rely on the variety of internal controls, including the management reports and other built in safe guards that will keep the program working. It may include the following things:

- Should allow the compliance officer(s) to recognize the deviations from internal controls and safety protocols;
- Should have the arrangements of dual controls where necessary;
- Should have arrangements of second review;

6.4. Establishment of Central Compliance Unit in the ICs

To ensure proper compliance of the provision laid down in the Money Laundering Prevention Act, 2009 each IC will establish system of internal monitoring through formation of a Central Compliance Unit (CCU) at the Head Office under the leadership of a high official and through nomination of a compliance officer at the branch/unit level of each IC. CCU will be under direct supervision of the Chief Executive Officer. In order to accomplish properly the jurisdiction and function of the CCU, each IC will formulate its Strategy and Program. CCU will issue the instructions to be followed by the branches/agencies. These instructions will be prepared combining the issues related to monitoring of transactions, internal control, policies and procedures from the point of preventing money laundering and terrorist financing.

6.4.1. Appointment of a Chief Anti Money Laundering Compliance Officer

All ICs must designate a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at its Head Office who has sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures and who will report directly to senior management and the board of directors. This provides evidence of senior management's commitment to efforts to combat ML/TF and, more importantly, provides added assurance that the officer will have sufficient clout to investigate potentially suspicious activities.

The position within the organization of the person appointed as CAMLCO will vary according to the size of the institution and the nature of its business, but he or she should be sufficiently senior to command the necessary authority. Each IC should prepare a detailed specification of the role and obligations of the CAMLCO. Larger ICs may choose to appoint

a senior member of their compliance, internal audit or inspection departments. In small institutions, it may be appropriate to designate the Head of Operations.

The CAMLCO may effect his or her responsibilities through a specific department, unit, group, or committee. Depending on the size, structure, business and resources of an IC, the designated department, unit, group, or committee or officer may be dedicated solely to the IC's AML/CFT responsibilities or perform the compliance functions in addition to existing duties.

The designated CAMLCO, directly or through the designated department, unit, group, or committee, should be a central point of contact for communicating with the regulatory agencies regarding issues related to the IC's AML/CFT program**s**.

Depending on the scale and nature of the institution the designated CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance while remaining responsible and accountable for the operation of the designated functions. In larger institutions, because of their size and complexity the appointment of one or more permanent Deputy CAMLCO of suitable seniority may be necessary.

The designated CAMLCO must ensure that at each division, region, branch or unit or agencies of the ICs that deal directly with the public, a senior level officer is appointed as Anti Money Laundering Compliance Officer (AMLCO) to ensure that each division, region, branch or agency is carrying out policies and procedures as required. These officers should report to the CAMLCO regularly on compliance issues and the need for any revisions to policies and procedures. This division, regional, branch, agency or unit level officers may be dedicated solely to the ICs anti money laundering responsibilities or perform the compliance functions in addition to existing duties.

All staff engaged in the IC at all levels must be made aware of the identity of the C*AMLCO,* his Deputy and the staffs, branch/agency level AMLCO, and the procedure to follow when making a suspicious activity report. All relevant staffs must be aware of the chain through which suspicious activity reports should be passed to the CAMLCO.

A sample job description of the Chief Anti Money Laundering Compliance Officer is given below for creating a suitable job description of the Regional/Branch/Agency/Unit Anti Money Laundering Compliance Officers (AMLCO):

Position Title: Chief Anti-Money Laundering Compliance Officer (CAMLCO)

Function: The Chief Anti Money Laundering Compliance Officer will report to the Chief Executive Officer. His/ Her responsibility will be to coordinate and monitor day to day compliance with applicable money laundering laws, rules and regulations; the Institution’s AML/CFT Policy (the “Policy”); and the practices, procedures and controls implemented by the Institution.

Position Responsibilities:

1) Monitor, review and coordinate application and enforcement of the IC's compliance policies including Anti-Money Laundering Compliance Policy. This will include an

AML/**CFT** risk assessment; and practices, procedures and controls for establishing of business relationship/policy sale, KYC procedures and ongoing transaction monitoring for detecting suspicious transactions/policy activity, and a written AML/**CFT** training plan;

2) Monitor changes of laws/regulations and directives of Bangladesh Bank that may require revisions to the Policy and making these revisions;

3) Respond to compliance questions and concerns of the staffs and advise regions/ branches/ agencies/ units and assist in providing solutions to potential issues involving compliance and ML/TF risks;

4) Ensure that the IC's AML/CFT Policy is complete and up-to-date; maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the IC;

5) Actively develop the compliance knowledge of all staff**s**, especially the compliance personnel. Develop and conduct training courses in the ICs to raise the level of awareness of compliance in the IC;

6) Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, Regional/ Branch/Agency/Unit Heads and compliance resources to assist in early identification of compliance issues;

7) Assist in review of control procedures in the IC to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;

8) Monitor the business' self-testing for AML/CFT compliance and any corrective action;

9) Manage the Suspicious Activity Reporting Process:

   - Review transactions and insurer's activities referred by divisional, regional, branch, agency or unit compliance officers as suspicious;
   - Review the Transaction Monitoring reports (directly or together with policy service personnel);
   - Ensure that internal Suspicious Activity Reports (internal SARs):
     - are prepared when appropriate;
     - reflect the uniform standard for "suspicious activity involving possible money laundering" established in the Policy;
     - are accompanied by documentation of the branch's decision to retain or terminate the policy contract as required under the Policy;
     - are advised to other branches of the institution who are known to have a relationship with the customer;
     - are reported to the chief executive officer and the board of directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .

- Ensure that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the Branch or Agency Manager;
- Maintain a review and follow up process to ensure that planned corrective action, including possible termination of policy, be taken in a timely manner;
- Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation;

Job Characteristics and Requirements

The Chief Anti Money Laundering Compliance Officer (CAMLCO) should possess:

- Proven leadership and organizational skills and ability to exert managerial control;
- Excellent communication skills, with an ability to clearly and diplomatically articulate issues, solutions and rationale; an effective trainer to raise the level of awareness of the control and compliance culture;
- Solid understanding of AML/CFT regulatory issues and product knowledge associated with a broad range of relevant financial services, banking activities and specially insurance services;
- High degree of judgment, good problem solving skills and be result oriented to ensure sound implementation of control and compliance processes and procedures;
- High personal standard of ethics, integrity and commitment to fulfilling the objectives of the position and protecting the interest of the IC.

The Chief Anti Money Laundering Compliance Officer (CAMLCO) must:

- Be familiar with the ways in which any of their respective business's products/policies and services may be abused by money launderers;
- Be able to assist their respective Institutions develop effective AML/CFT policies, including programs to provide AML/CFT training to all personnel;
- Be able to assist their respective business assess the ways in which products under development may be abused by money launderers in order to establish appropriate AML/CFT controls before product is rolled out into the marketplace.
- Be capable of assisting their respective business evaluate whether questionable activity is suspicious under the standard set forth in the AML/CFT Policy and under any applicable law and regulation;
- Attend each year at least one formal AML/CFT training program, either internal or external;

Education (or Equivalent Training)

The CAMLCO should have a working knowledge of the diverse insurance products offered by the Institution. The person could have obtained relevant insurance business and compliance experience as an internal auditor or regulatory examiner, with exposure to

different Insurance business products and businesses. Product and insurance related knowledge could be obtained from being an external or internal auditor, or as an experienced operations staff.

Experience

CAMLCO should have a minimum of ten years of experience, with a minimum of three years at a managerial/administrative level.

6.5 Ongoing Employee Training and Awareness Program

FATF recommendation 15 suggests that a formal AML/CFT compliance program should include an ongoing employee training program. The importance of a successful training and awareness program should not be overstated. Employees in different business functions need to understand how the institution's policy, procedures, and controls affect them in their day to day activities.

Statutory Requirements

Section 23 (cha) of the Money Laundering Prevention Act, 2009 requires Bangladesh Bank to provide training to the staff/officers of ICs, financial institutions and other institutions engaged in financial activities in order to combat money laundering.

Since ICs themselves have responsibilities under the Act in relation to identification, reporting and record retention, it follows that they must ensure that their staffs are adequately trained to discharge their responsibilities.

It is therefore imperative for all ICs to take appropriate measures to make employees aware of:

- policies and procedures to prevent money laundering and combating financing of terrorism and for identification, record keeping and internal reporting;
- the legal requirements; and
- to provide relevant employees with training in the recognition and handling of suspicious transactions.

The Act does not specify the nature of the training to be given and these Guidance Notes therefore set out what steps might be appropriate to enable institutions to fulfill this requirement.

The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in the Guidance Notes must depend on the extent to which the staff of institutions appreciates the serious nature of the background against which the legislation has been enacted. The Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions.

It is, therefore, important that ICs introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

Education and Training Programs

Timing and content of training packages for various sectors of staff will need to be adapted by individual businesses for their own needs. However, it is recommended that the following might be appropriate.

All relevant staff should be educated in the process of the "know your customer" requirements for AML/CFT. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's/ insured's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some form of high-level general awareness raising training is therefore suggested.

6.5.1 What to train

An effective training program should include:

- General information of the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT laws apply to ICs and their employees;
- Institution's policies and systems with regard to customer identification and verification, due diligence , monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees.
- The person responsible for designing the training must identify which, if any, of these topics relate to the target audience.
- Effective training should present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on the institution.

6.5.2 Whom to train

Training should be provided in the following categories:

New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Anti Money Laundering Compliance Officer (AMLCO) should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

Front-line Staff

Members of staff who are dealing directly with the public or customer or potential policy buyer are the first point of contact with potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

Processing (Back Office) Staff

Those who sell policies and fill up the forms of that policy, receive premiums and pay the claims must receive appropriate training for processing those activities. In addition, they must have training to verify the identity of the customers, their sources of income and to identify the beneficial owners of the policy. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti-Money Laundering Compliance Officer whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

Audit and compliance staff

These are the people charged with overseeing, monitoring and testing money laundering controls, and they should be trained about changes in regulation, money laundering methods and enforcement and their impact on the institution.

Senior Management, Operation Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Act for non-reporting and for assisting money launderers; internal reporting procedures and the requirements for verification of identity and the retention of records.

Board of Directors

Money laundering and terrorist financing issues and dangers should be regularly and thoroughly communicated to the board of directors. It is important that the compliance department has strong board support and one way to ensure that is to keep board members aware of the reputational risk that money laundering poses to the institution.

Anti Money Laundering Compliance Officer

In depth training on all aspects of the Money Laundering and Terrorist Financing Legislation, Bangladesh Bank directives and internal policies will be required for the Anti Money Laundering Compliance Officer. In addition, the AMLCO will require extensive instructions on the validation and reporting of suspicious transactions and suspicious activities and on the feedback arrangements and on new trends and patterns of criminal activities.

6.5.3 How to train

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed. e.g. uncovered issues by audits or exams, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly in case of a case study used to illustrate appoint, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee personnel file should be recorded accordingly.
- Refresher Training: In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some financial sector

businesses may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

- Training should be ongoing, incorporating trends and developments in an institution's business risk profile, as well as changes in the AML/CFT legislation. Training on new money laundering schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

6.6 Independent Audit Function

6.6.1 Why the audit function is necessary

To ensure the effectiveness of AML/CFT program, IC should assess the program regularly and look for new risk factors. FATF recommendation 15 suggests that institutions covered by AML/CFT laws should establish and maintain policies, procedures and controls which should include an appropriate compliance function and an audit function.

6.6.2 Why the audit function must be independent

The audit must be independent (i.e. performed by people not involved with the IC's AML/CFT compliance staff). Audit is a kind of assessment of checking of a planned activity. Those who do not have any stance in the company will check or examine the entity objectively. To ensure objective assessment it is important to engage an independent body to do any audit.

6.6.3 Whom they will report

The individuals conducting the audit function should report directly to the board of directors/senior management.

6.6.4 The ways of performing audit function

Audit function shall be done by the internal auditors. At the same time external auditors might be appointed to review the adequacy of the program.

6.6.4.1 Internal audit

An institution's internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The internal audit should

- Address the adequacy of AML/CFT risk assessment
- Examine/attest the overall integrity and effectiveness of the management systems and the AML/CFT control environment
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.

- Determine personnel adherence to the IC's AML/CFT policies, procedures and processes.
- Perform appropriate testing procedure with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the IC's processes for identifying and reporting suspicious activity.
- Where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check.
- Communicate the findings to the board and/or senior management in a timely manner
- Recommend corrective action for deficiencies
- Track previously identified deficiencies and ensure management corrects them
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Determine when assessing the training program and materials:
  - The importance the board and the senior management place on ongoing education, training and compliance;
  - Employee accountability for ensuring AML/CFT compliance;
  - Comprehensiveness of training, in view of specific risks of individual business lines;
  - Training of personnel from all applicable areas of the IC;
  - Frequency of training;
  - Coverage of IC policies, procedures, processes and new rules and regulations;
  - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity; and
  - Penalties for noncompliance and
  - Regulatory requirements.

6.6.4.2 External audit

External auditor may play an essential part in reviewing the adequacy of AML/CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit risk-focus their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. This external audit might be conducted by the external auditor as a part of statutory financial audit. External auditors may report incidents of suspected criminal activity uncovered during audits, to the financial sector supervisors.

6.7 Control measures and procedures

Insurers should be constantly vigilant in deterring criminals from making use of them for the purposes of money laundering or the financing of terrorism. By understanding the risks of money laundering and the financing of terrorism, insurers are in a position to determine what can be done to control these risks and which procedures and measures can be implemented effectively and efficiently.

For reasons of sound business practice and proper risk management, insurers should have controls in place to assess the risks of each business relationship. As customer due diligence is a business practice suitable not just for commercial risk assessment and fraud prevention but also to prevent money laundering and the financing of terrorism, control measures should be linked to these existing controls. The concept of customer due diligence goes beyond the identification and verification of only the policyholder – it extends to identification of the potential risks of the whole business relationship.

The duty of vigilance consists mainly of the following elements:

- customer due diligence and verification of identity;
- recognition and reporting of suspicious customers/transactions, and
- provisions affecting the organization and the staff of the insurer, such as a compliance and audit environment, keeping of records, the recruitment of staff and training.

Chapter 7: Identification Procedures

7.1 Performing Due Diligence on Customers/ Beneficial Owners/ Beneficiaries

Insurers should know the customers with whom they are dealing. A first step in setting up a system of customer due diligence is to develop clear, written and risk based client acceptance policies and procedures, which among other things include the types of products offered in combination with different client profiles. These policies and procedures should be built on the strategic policies of the board of directors of the insurer, including policies on products, markets and clients.

The insurer's strategic policies will determine its exposure to risks such as underwriting risk, reputational risk, operational risk, concentration risk and legal risk. After determining the strategic policies, client acceptance policies should be established, taking into account of the risk factors such as the background of the customer and/or beneficial owner and the complexity of the business relationship. This is why – as indicated above – control measures and procedures with respect to AML/CFT should be an integral part of the overall customer due diligence.

Insurers should be aware that they are more vulnerable to ML/TF if they sell short term coverage by means of a single premium policy than if they sell group pensions to an employer with annuities to be paid after retirement. The former is more sensitive to ML/TF and therefore calls for more intensive checks on the background of the client and the origin of the premium than the latter. Insurers should also be aware of requests for multiple policies to be taken out for premiums slightly below any publicized limits for performing checks, such as checks on the source of wealth.

7.1.1 Customer Due Diligence Measures

Customer due diligence measures that should be taken by insurers include:

- identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information
- determining whether the customer is acting on behalf of another person. If so then the reasonable steps should be taken to obtain sufficient identification data to verify the identity of the person behind.
- identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements insurers should take reasonable measures to understand the ownership and control structure of the customer
- obtaining information on the purpose and intended nature of the business relationship and other relevant factors
- 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 insurer's knowledge of the

customer and/or beneficial owner, their business and risk profile, including, where necessary, the source of funds.

The extent and specific form of these measures may be determined following a risk analysis based upon relevant factors including the customer, the business relationship and the transaction(s). Enhanced due diligence is called for with respect to higher risk categories. Decisions taken on establishing relationships with higher risk customers and/or beneficial owners should be taken by senior management. Subject to legal requirements, insurers may apply reduced or simplified measures in the case of low risk categories.

Prior to the establishment of a business relationship, the insurer should assess the characteristics of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this assessment, the insurer should decide whether or not to accept the business relationship. As a matter of principle, insurers should not offer insurance to customers or for beneficiaries that obviously use fictitious names or whose identity is kept anonymous.

Factors to consider when assessing risks, which are not set out in any particular order of importance and which should not be considered exhaustive, include (where appropriate):

- type and background of customer and/or beneficial owner
- the nature of the activities
- the means of payment as well as the type of payment (cash, or other means of payment)
- the source of funds
- the source of wealth
- the frequency and scale of activity
- the type and complexity of the business relationship
- whether or not payments will be made to third parties
- whether a business relationship is dormant
- suspicion or knowledge of money laundering, financing of terrorism or other crime.

The requirements for customer due diligence should apply to all new customers as well as − on the basis of materiality and risk − to existing customers and/or beneficial owners. As to the latter the insurer should conduct due diligence at appropriate times. In insurance, various transactions or ‘trigger events’ occur after the contract date and indicate where due diligence may be applicable. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries.

The requirement for an insurer to pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose is essential to both the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. In this respect “transactions” should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

In the event of failure to complete verification of any relevant verification subject or to obtain information on the purpose and intended nature of the business relationship, the insurer should not conclude the insurance contract, perform the transaction, or should terminate the business relationship. The insurer should also consider making a suspicious transaction report (STR) to the financial intelligence unit (FIU).

7.1.2 Enhanced measures with respect to higher risk customers and non-cooperative countries and territories

Enhanced CDD measures should apply to all higher risk business relationships, clients and transactions and non-cooperative countries and territories (NCCTs). Jurisdictions that do not sufficiently apply the FATF Recommendations could be listed by the FATF as NCCTs. In specific circumstances, jurisdictions may be asked to impose appropriate countermeasures. Insurers should give special attention, especially in underwriting and claims settlement, to business originating from jurisdictions which do not sufficiently apply the FATF Recommendations. This includes both high risk business relationships assessed by the insurer, based on the customer's individual risk situation, and the types of business relationships.

With regard to enhanced due diligence, in general the insurer should consider which of the following, or possible additional measures, are appropriate:

- certification by appropriate authorities and professionals of documents presented
- requisition of additional documents to complement those which are otherwise required
- performance of due diligence on identity and background of the customer and/or beneficial owner, including the structure in the event of a corporate customer
- performance of due diligence on source of funds and wealth
- obtaining senior management approval for establishing business relationship
- conducting enhanced ongoing monitoring of the business relationship.

7.1.3 Politically exposed persons

The FATF Recommendations require additional due diligence measures in relation to PEPs. For this purpose insurers should:

- have appropriate risk management systems to determine whether the customer is a PEP. The board of directors of the insurer must establish a client acceptance policy with regard to PEPs, taking account of the reputational and other relevant risks involved.
- obtain senior management approval for establishing business relationships with such customers
- take reasonable measures to establish the source of wealth and source of funds, and
- conduct enhanced ongoing monitoring of the business relationship.

7.1.4 New or developing technologies

New or developing technologies can be used to market insurance products. E-commerce or sales through the internet is an example of this. Although for this type of non-face-to-face business verification may be allowed after establishing the business relationship, the insurer should nevertheless complete verification.

Although a non-face-to-face customer can produce the same documentation as a face-to-face customer, it is more difficult to verify their identity. Therefore, in accepting business from non-face-to-face customers an insurer should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.

Examples of such risk mitigating measures are:

- certification by appropriate authorities and professionals of the documents provided
- requisition of additional documents to complement those which are required for face-to-face customers
- independent contact with the customer by the insurer
- third party introduction, e.g. by an intermediary subject to the criteria established
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

7.1.5 Simplified customer due diligence

In general, the full range of CDD measures should be applied to the business relationship. However, if the risk of money laundering or the financing of terrorism is lower (based on the insurer's own assessment), and if information on the identity of the customer and the beneficial owner is publicly available, or adequate checks and controls exist elsewhere in national systems it could be reasonable for insurers to apply, subject to national legislation, simplified or reduced CDD measures when identifying and verifying the identity of the customer, the beneficial owner and other parties to the business relationship.

Insurers should bear in mind that the FATF lists the following examples of customers where simplified or reduced measures could apply:

- financial institutions – where they are subject to requirements to combat money laundering and the financing of terrorism consistent with the FATF Recommendations, and are supervised for compliance with those controls
- public companies that are subject to regulatory disclosure requirements
- government administrations or enterprises.

Furthermore, the FATF states that simplified CDD or reduced measures could also be acceptable for various types of products or transactions such as (examples only):

- insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral

- a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

If the Micro Insurance policies have the annual premium of no more than Taka10,000.00, the ICs may apply simplified CDD for their policyholders.

7.1.6 Reliance on intermediaries and third parties

It is allowed to rely on intermediaries and third parties to perform the following CDD elements:

- identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information
- identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner to the extent the intermediary or third party is satisfied that they know who the beneficial owner is, including taking reasonable measures to understand the ownership and control structure of the customer, and
- obtaining information on the purpose and intended nature of the business relationship.

However, the following criteria should be met:

- the insurer should immediately obtain the necessary information concerning the above mentioned elements. Insurers should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the intermediaries and third parties upon request without delay. Insurers should be satisfied with the quality of the due diligence undertaken by the intermediaries and third parties.
- the insurer should satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with CDD requirements in line with FATF Recommendations 5 and 10.

The ultimate responsibility for customer and/or beneficial owner identification and verification remain with the insurer relying on the intermediaries or third parties. The checks by the insurer as indicated in the previous paragraph do not have to consist of a check of every individual transaction by the intermediary or third party. The insurer should be satisfied that the AML and CFT measures are implemented and operating adequately.

Insurers should satisfy the above provisions by including specific clauses in the agreements with intermediaries/third parties or by any other appropriate means. These clauses should include commitments for the intermediaries/third parties to perform the necessary CDD measures, granting access to client files and sending (copies of) files to the insurer upon request without delay. The agreement could also include other compliance issues such as reporting to the FIU and the insurer in the case of a suspicious transaction. It is recommended that insurers use application forms to be filled out by the customers and/or intermediaries/third parties that include information on identification of the customer and/or beneficial owner as well as the method used to verify their identity.

The insurer should undertake and complete its own verification of the customer and beneficial owner if it has any doubt about the ability of the intermediary or the third party to undertake appropriate due diligence.

7.2 Know Your Customer Profile

To combat attempts by money launderers and terrorist financers from using Non-life insurance business there is a need for every general insurance business to use the **"Know Your Customer"** principle in their day-to-day business activities.

The overriding requirement behind the principle of KYC is to establish the identity of the party(ies) wishing to create a business relationship. This applies equally wherever the applicant may be based and whether the applicant is an individual, company, trust, nominee or other.

"Know your Customer" principles do not infringe on the confidentiality and privacy of client affairs.

Before a business relationship is established all insurance business must satisfy themselves as to the identity of the applicant for a business Relationship. In the absence of satisfactory evidence, the Application of a business relationship shall not proceed any further.

The ICs must hold either original documents, or suitably certified copies of original documents of identification, on its files.

It should be noted that it is not possible for insurance company to delegate the responsibility of know your customs to another party: however in certain circumstances it is acceptable for the collection of the identity documents to be delegated.

7.2.1 Sound Know Your Customer (KYC) procedures

Sound Know Your Customer (KYC) procedures are critical elements in the effective management of insurance risks. KYC safeguards go beyond simple policy issuing and recordkeeping and require insurance companies to formulate a customer acceptance policy and a tiered customer identification program that involves more extensive due diligence for higher risky policyholders and includes proactive underwriting procedure for suspicious activities.

Sound KYC procedures have particular relevance to the safety and soundness of insurance companies, in that:

- they help to protect insurance company's reputation and the integrity of insurance systems by reducing the likelihood of insurance companies becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets covered by insurance policy).

7.2.2 The Inadequacy or Absence of KYC Standards

The inadequacy or absence of KYC standards can subject insurance companies to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to insurance companies (e.g. through the cancellation of insurance policies, fraudulent claims, investigation costs, asset seizures and freezes, and other losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

- Reputational risk poses a major threat to ICs, since the nature of their business requires maintaining the confidence of clients/insured's and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding an insurance company's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. ICs are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC program. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.
- Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of ICs' programs, ineffective control procedures and failure to practice due diligence. A public perception that an IC is not able to manage its operational risk effectively can disrupt or adversely affect the business of the IC.
- Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of an IC. ICs may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, ICs can, for example, suffer fines, criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving an IC may have far greater cost implications for its business than just the legal costs. ICs will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.
- On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden cancellation of policies, with potentially damaging consequences for the ICs' liquidity. Funding risk is more likely to be higher in the case of small insurance companies and those that are less active in the wholesale markets than large insurance companies. Analyzing underwriting concentrations requires ICs to understand the characteristics of their clients, including not only their identities but also the extent to which their actions may be linked with those of other clients.

7.2.3 Know Your Customer (KYC) Policies and Procedures

Having sufficient information about the customer - "knowing your customer" (KYC) - and making use of that information underpins all anti-money laundering efforts, and is the most effective defense against being used to launder the proceeds of crime. If a customer has established relationship using a false identity, s/he may be doing so to defraud the institution itself, or to ensure that s/he cannot be traced or linked to the crime the proceeds of which the institution is being used to launder. A false name, address or date of birth will usually mean that law enforcement agencies cannot trace the customer if s/he is needed for interview as part of an investigation.

All institutions are to seek satisfactory evidence of the identity of those with whom they deal (referred to in these Guidance Notes as verification of identity). Unless satisfactory evidence of the identity of potential customers is obtained in good time, the business relationship must not proceed.

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. **In order to be able to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried on by their customers.**

An institution must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.

The verification procedures needed to establish the identity of a prospective customer should basically be the same whatever be the type of policy or service required. The best identification documents possible should be obtained from the prospective customer. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity. So verification will generally be a cumulative process. **The overriding principle is that every institution must know who their customers are, and have the necessary documentary evidence to verify this.**

ICs in the design of KYC programs should include certain key elements. Such essential elements should start from the ICs' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk clients and (4) identification of suspicious transactions. ICs should not only establish the identity of their customers, but should also monitor policy activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of policy. KYC should be a core feature of insurance companies' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

The intensity of KYC programs beyond these essential elements should be tailored to the degree of risk.

7.2.4 Document in KYC process

Insurance companies are required to collect

- Recent photograph of individual client
- Document identity of the customer (National ID, Passport, Birth Registration Certificate or driving license)
- His/her residential address (both present and permanent),
- Sources of funds based on the risk profile of the customer,
- Besides, documents required by risk underwriting norms.

7.3 Customer Acceptance Policy

ICs should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to an IC. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked policies, business activities or other risk indicators should be considered.

ICs should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic underwriting requirements for a working individual with a small sum insured. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to insurance services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds are unclear. Decisions to enter into business relationships with higher risk customers such as public figures or politically exposed persons should be taken exclusively at senior management level.

Where the insurer believes (beyond reasonable grounds) that the applicant for the business relationship is an acceptable applicant, the acceptable applicant may be accepted without defaulted identification and verification efforts being made. The IC should record in detail on the client file the basis on which the acceptable applicant has been accepted. If the evidence is not provided by the acceptable applicant the insurer must either obtain the evidence themselves or obtain satisfactory evidence from on alternative source.

7.4 Establishing a Business Relationship

Before an insurance contract is concluded between customer and insurer, there is already a pre-contractual business relationship between these two and possibly other parties. After a policy is taken out:

- the insurer covers a certain risk described in the contract and policy conditions
- certain transactions may take place such as premium payments, payments of advance or final benefits, and
- certain events may occur such as a change in cover or a change of beneficiaries.

The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. To achieve this, the insurer will collect relevant information, for example details of source of funds, income, employment, family situation, medical history, etc. This will lead to a customer profile which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events.

The insurer should realize that creating a customer profile is also of importance for AML/CFT purposes and therefore for the protection of the integrity of the insurer and its business.

In addition, the beneficial owner should also be identified and verified. For the purposes of this guidance paper, the expression beneficial owner applies to the owner/controller of the policyholder as well as to the beneficiary to the contract.

With regard to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policyholder and the reinsurance company, it is often impractical or impossible for the reinsurer to carry out verification of the policyholder or the beneficial owner. Therefore, for reinsurance business reinsurers should only deal with ceding insurers (1) that are licensed or otherwise authorized to issue insurance policies and (2) which have warranted or otherwise confirmed that they apply AML/CFT standards at least equivalent to those in this guidance paper, provided there is no information available to the contrary for instance from FATF and trade associations or from the reinsurers' visits to the premises of the insurer.

When the identity of customers and beneficial owners with respect to the insurance contract has been established the insurer is able to assess the risk to its business by checking customers and beneficial owners against internal and external information on known fraudsters or money launderers (possibly available from industry databases) and on known or suspected terrorists (publicly available on sanctions lists such as those published by the United Nations). The IAIS recommends that insurers use available sources of information when considering whether or not to accept a risk. Identification and subsequent verification will also prevent anonymity of policyholders or beneficiaries and the use of fictitious names.

Transactions and events in the course of the business relationship:

The insurer should perform ongoing due diligence on the business relationship. In general, the insurer should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. Enhanced due diligence is required with respect to higher risk categories. The CDD program should be established in a way that the insurer is able to adequately gather and analyze information.

Examples of transactions or trigger events after establishment of the contract that require CDD are:

- a change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to persons other than beneficiaries)
- a change/increase of insured capital and/or of the premium payment (for instance, which appear unusual in the light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party)
- use of cash and/or payment of large single premiums
- payment/surrender by a wire transfer from/to foreign parties
- payment by banking instruments which allow anonymity of the transaction
- change of address and/or place of residence of the policyholder, in particular, tax residence
- lump sum top-ups to an existing life insurance contract
- lump sum contributions to personal pension contracts
- requests for prepayment of benefits
- use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution)
- change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment)
- early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief)

The above list is not exhaustive. Insurers should consider other types of transactions or trigger events which are appropriate to their type of business.

Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurer is entitled to rely on this unless doubts arise about the veracity of that information it holds. As an example, doubts might arise if benefits from one policy of insurance are used to fund the premium payments of another policy of insurance.

7.5 Customer Identification

Customer identification is an essential element of KYC standards. For the purposes of this Guidance Notes, a customer includes:

- the person or entity that maintains an insurance policy with the company or those on whose behalf an insurance policy is taken (i.e. beneficial owners);
- the beneficiaries of insurance policy conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the insurance companies.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for ICs to undertake regular reviews of existing records. An appropriate time to do so is when customer documentation standards change substantially, or when there is a material change in the way that the policy is operated. However, if an IC becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained and information should be updated or reviewed as appropriate.

7.5.1 Timing of Identification

In principle, identification and verification of customers and beneficial owners should take place when the business relationship with that person is established. This means that (the owner / controller of) the policyholder needs to be identified and their identity verified before, or at the moment when, the insurance contact is concluded. Valid exceptions are mentioned in the following paragraphs.

Identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the money laundering risks and financing of terrorism risks are effectively managed. However, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

Where a policyholder and/or beneficiary is permitted to utilize the business relationship prior to verification, ICs should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. Where the insurer has already commenced the business relationship and is unable to comply with the verification requirements, it should terminate the business relationship and consider making a suspicious transaction report.

Examples of situations where a business relationship could be used prior to verification are:

- group pension schemes
- non-face-to-face customers
- premium payment made before the application has been processed and the risk accepted, and
- using a policy as collateral.

In addition, in the case of non-face-to-face business, verification may be allowed after establishing the business relationship. However, insurers must have policies and procedures in place to address the specific risks associated with non-face-to-face business relationships and transactions.

7.5.2 Methods of Identification and Verification

This guidance paper does not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. It does set out what, as a matter of good practice, may reasonably be expected of insurers. Since, however, this guidance paper is neither mandatory nor exhaustive; there may be cases where an insurer has properly satisfied itself that verification has been achieved by other means the one which it can justify to the appropriate authorities as reasonable in the circumstances.

The best possible identification documentation should be obtained from each verification subject. "Best possible" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

7.5.2.1 What Constitutes a Person's Identity

Identity generally means a set of attributes which uniquely define a natural or legal person.

There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership, etc). For the purposes of this guidance, the two elements are:

- the physical identity (e.g. name, date of birth, TIN/voter registration/passport/National ID, etc.); and
- the activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

When commencing a business relationship, institutions should consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. Documentation about the nature of the applicant's business should cover the origin of funds to be used for premium payment.

Once a policy is issued, reasonable steps should be taken by the IC to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process do not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or

service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

So a person's identity constitutes

a. Full name
b. Unique identification number
c. Existing residence address
d. Contact telephone number
e. Date of Birth / Birth certificate
f. Nationality

7.5.2.2 Individual Customers

Where verification of identity is required, the following information should be obtained from all individual applicants for issuing insurance policy or other relationships, and should be verified by the insurance company itself:

- true name and/or names used;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income

One or more of the following options are recommended to verify identity of the prospective policy buyer.

- consult with a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- consult with national identity card;
- checking the telephone directory;
- record of home/office visit.

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that an institution does not breach UN or other international financial sanctions.

Identification documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:-

(i) Current valid passport;

(ii) National ID Card;

(iii) Valid driving license;

(iv) Employer's ID card;

(v) Birth Registration Certificate

(vi) A Bangladeshi employer ID card bearing the photograph and signature of the applicant; or

(vii) A certificate from any local government organs such as Union Council chairman, Ward Commissioner, etc. or any respectable person acceptable to the insurance company.

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as **sole** evidence of identity, e.g. birth certificate, credit cards, non- Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. ICs should also be aware of the authenticity of passports.

Where there is no **face-to-face contact**, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity.

At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID Card where there is no face-to-face contact, then a certified true copy should be obtained.

There is obviously a wide range of documents which might be provided as evidence of identity.

It is for each institution to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

In respect of joint policy where the surname and/or address of the policy holders differ, the name and address of all policy holders, not only the first named, should normally be verified in accordance with the procedures set out above.

Any subsequent change to the policy holder's name, address, or employment details of which the IC becomes aware should be recorded as part of the know your customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for AML/CFT.

7.5.2.3 File copies of supporting evidence should be retained

Where this is not possible, the relevant details should be recorded on the applicant's file. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record identification details on a separate form.

An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach policy issuing procedures as a favor to an applicant

7.5.2.4 Persons without Standard Identification Documentation

Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to have so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended.

Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

In these cases it may be possible for the institution to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person’s address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer’s file, and must also retain this information in the same manner and for the same period of time as other identification records.

For students or other young people, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant’s educational institution.

Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person purchasing the policy is not already known, the identity of that person, and any other person who will have control of the policy, should be verified.

7.5.2.5 Corporate Bodies and other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. **The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company.** Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh.

Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified true copy of the Memorandum and Articles of Association, or by-laws of the client;
- Copy of the board resolution to purchase the group insurance policy and the empowering authority for those who will operate any policy;

- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the policy related documents are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the signatories of policy related documents, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the reason for using the second name makes sense.

The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:

- All of the directors who will be responsible for the operation of the policy/transaction.
- All the authorized signatories for the policy/transaction.
- All holders of powers of attorney to operate the policy/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

7.5.2.6 Partnerships and Unincorporated Businesses

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the purchase of a policy and conferring authority on those who will operate it should be obtained.

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

7.5.2.7 Powers of Attorney/ Mandates to Operate Policies

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

7.5.2.8 Requirements of Policies Commenced Prior to 15 April 2008

Anti money laundering legislation and requirements in respect of KYC procedures for business relationships did not apply prior to 15th April 2008 for ICs. It is therefore reasonable to assume that business relationships commenced before that date may not satisfy the requirements of these guidance notes in terms of supporting documentary evidence. In some circumstances, the lack of up to date documentary evidence to support existing business relationships may pose operational and other risks to the ICs. Consequently, all relevant financial businesses must review existing business relationships commenced prior to 15th April 2008 (referred to in this section as "pre 2008 policies") to establish whether any documentary evidence required by their current KYC procedures is lacking.

7.6 Timing and Duration of Verification

The best time to undertake verification is *prior to entry* into the relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.

However, if it is necessary for sound business reasons to issue a policy or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties.

Alternatively, a senior member of staff may give appropriate authority.

This authority should not be delegated, and should only be done in exceptional circumstances.

Any such decision should be recorded in writing.

Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is in itself suspicious.

7.7 Record Keeping

ICs must preserve record of transaction with all necessary documents for a period of at least five years from the date of closing any account or cancellation of any Policy/closing on maturity/rejection of any policy

Chapter 8: Meaning, Importance, obligation and nature of STR/SAR

The final output of all AML/CFT compliance program is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the ML/FT risks of reporting agencies including ICs. So, establishment of a mechanism to detect STR/SAR and reporting such to the competent Authority is necessary for the safety and soundness of the insurance sector.

8.1 What is STR/SAR

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there is a reasonable ground to believe that funds are the proceeds of crime or may be linked to terrorist activity or the transactions do not seem to be usual. Such unusual activities or transactions must be reported to competent authorities. Herein the competent authority refers to Bangladesh Bank as per Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009. In the section (2)(n) of Money Laundering Prevention Act, 2009 **"suspicious transaction"** means transactions-

(i) that substantially deviates from the usual transaction;

(ii) that have reasonable grounds to suspect that the transactions have involvement with any proceeds of crime;

As per Anti Terrorism Act, 2009, STR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. Important thing is that ICs need not establish any proof of occurring a predicate offence before reporting STR/SAR; they must submit STR/SAR only on the basis of suspicion.

8.2 Obligations of STR/SAR

According to the provision laid down in the section 25(1)(d) of Money Laundering Prevention Act, 2009, reporting agencies (including ICs) are obligated to submit STR/SAR to the Bangladesh Bank spontaneously. Anti Money Laundering Department of Bangladesh Bank has also instructed the ICs to submit STR/SAR through AML Circular No. 18 circulated with the purview of the legislation mentioned above.

8.3 Importance of STR/SAR

As discussed above, STR/SAR is very crucial for the safety and soundness of the ICs. The ICs should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect the reputation of ICs;
- It helps to protect ICs from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate financial crimes related to money laundering, terrorist financing.

8.4 STR/SAR Identification and Reporting Procedure

It is very important for ICs to establish an effective identification system of STR/SAR to mitigate the AML/CFT risk of that institution. ICs must have in place an efficient detection mechanism to identify STR/SAR. When any transaction related to a policy seems to be suspicious in terms of the nature, activity, volume, complexity etc., or significantly mismatch with customer declared information the concerned officer should apply his/her prudence on it. If he/she dose not get satisfactory answer, after evaluation it should be reported or recorded. Note that suspicion may not arise only at the time of transaction but also at the time of completing KYC and attempted transaction. In case of reporting of STR/SAR, ICs should undertake the following stages:

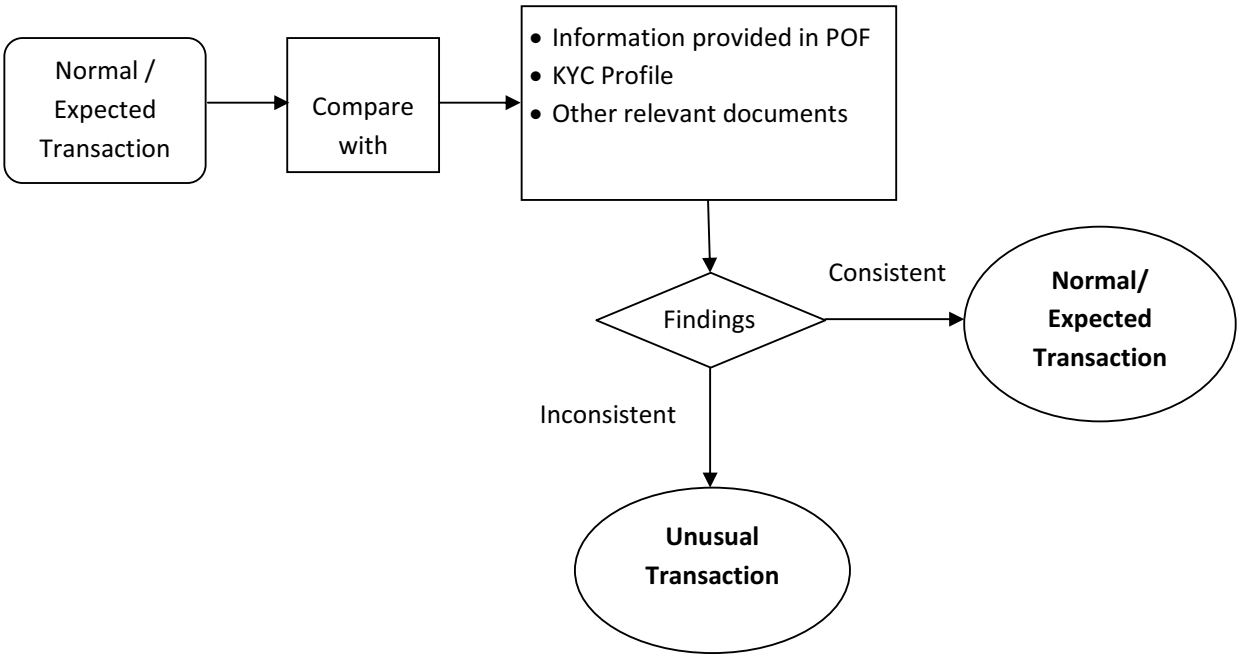
8.4.1 Identification of STR/SAR

Identification of STR/SAR starts from identifying unusual transaction and activity. Such unusual transaction may be unusual in terms of nature of transaction, volume of transaction, complexity of transaction, timing of transaction etc. Generally, something unusual may be detected while:

- Transactions are found inconsistent with the KYC profile and there is no valid reasonable explanation;
- Monitoring customer transactions;
- Using red flag indicator;

This stage is very vital for reporting of STR/SAR. Depending on size, need and complexity of ICs, monitoring of unusual transactions may be automated, manual or both. Some ICs use specialized software to detect unusual transactions or activities, however, the use of such software can only complement managerial oversight and not replace the need for constant monitoring of the policy of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution regarding product, customer etc. and supported by adequate information systems to alert management and other appropriate staff (e.g., the AML/CFT compliance officer) of unusual /suspicious activity. A STR/SAR may be identified at any desk or by any officer noticing the customer's unusual transaction or activity. For that reason training of staff to identify unusual /suspicious transaction/activity should always be an ongoing activity.

The flow chart below shows the identification process of STR/SAR. For Simplification, if any transaction/activity consistent with the information provided by the customer treated as normal & expected. When such transaction/activity is not normal & expected, it may treat as unusual transaction/activity.



Flow chart: The identification process of Unusual/Suspicious Transaction/Activity

As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity.

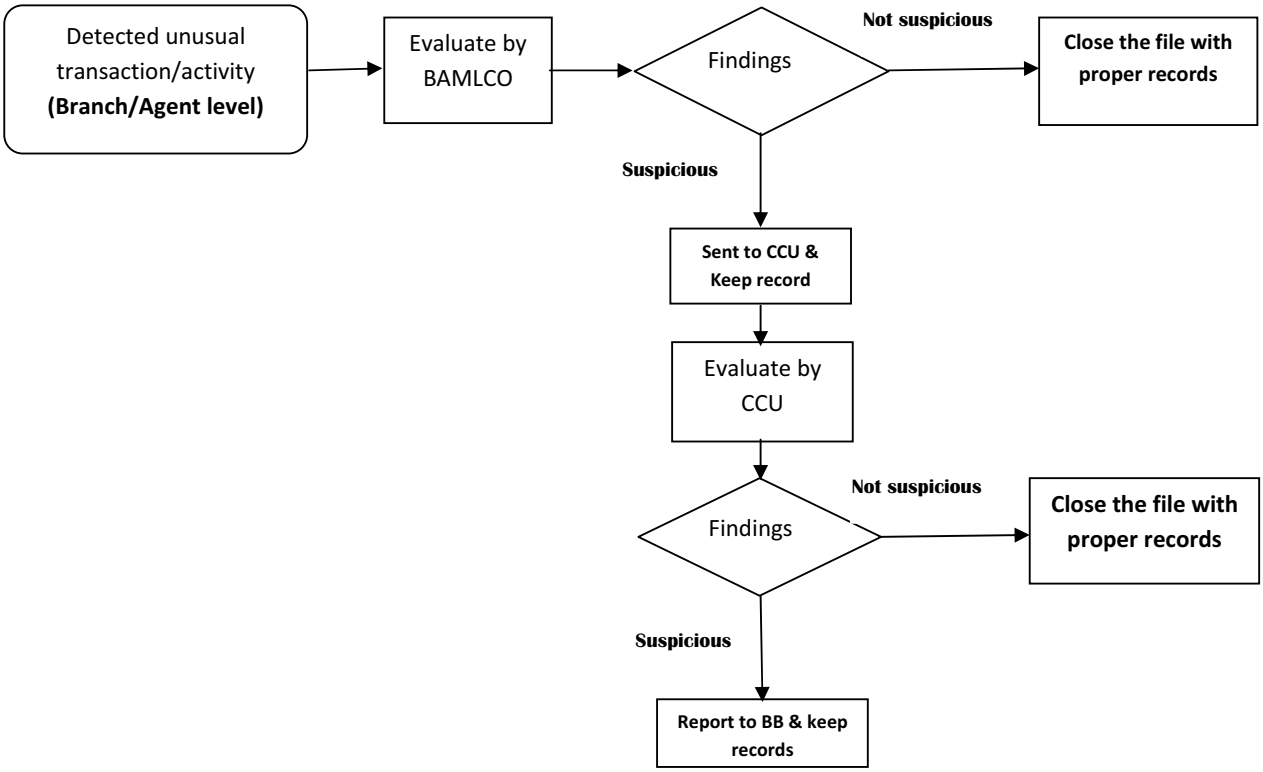
8.4.2 Evaluation of Unusual/Suspicious Transaction/Activity

This stage must be in place at branch/agent/operational level and Central Compliance Unit (CCU) of an IC. After identification of Unusual/Suspicious Transaction/Activity, at branch /agent level Branch/Agent Anti Money Laundering Compliance Officer should evaluate the transaction/activity to identify suspicion by interviewing the customer, collecting supporting documents any other ways. If Branch/Agent Anti Money Laundering Compliance Officer is not satisfied or it seems still suspicious, he/she should forward the report to CCU. After receiving report from branch CCU should also evaluate the report whether the STR/SAR has sufficient merit for submission to Bangladesh Bank. Records relating to such transactions must be maintained even for those cases which would not be submitted to BB.

8.4.3 Disclosure of STR/SAR

This is the final stage of reporting STR/SAR. In due course, if the transaction/activity found suspicious, CCU should report it to Bangladesh Bank immediately.

For simplification, the outlined flow chart given below shows STR/SAR identification and reporting procedures at a glance:



Flow chart: Identification and Reporting Procedures of STR/SAR

8.4.4 When and Where to report

ICs should ensure appropriate timing of submitting suspicious transaction report to mitigate AML/CFT risk. The timing of report differs with respect to nature of STR/SAR.

1. Any suspicious transaction/activity related to money laundering must be reported within 5 days of detection.
2. Any suspicious transaction/activity related to terrorist financing must be reported within the 3 days of detection.

All report should be sent to:

General Manager
Anti Money Laundering Department
Bangladesh Bank, Head Office
Motijheel, Dhaka.
Phone: +88 02 7120659
Fax: +88 02 7120371

8.5 Things to consider in detecting STR/SAR

ICs must consider the following questions while seeking to identify a suspicious transaction:

(a) Is the customer known personally?

(b) Is the transactions in keeping with the customer's normal activity known to the markets in which the customer is active and the customer's own business i.e. does the transaction make sense?

(c) Is the transaction in keeping with normal practice in the market (i.e. with reference to market, size and frequency) to which it relates?

(d) Is the role of the agent involved in the transaction unusual?

(e) Is the transaction to be settled following normal manner?

(f) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?

(g) Are the reasons for the transaction bear economic sense i.e. might there be an easier, cheaper or more convenient method available?

(h) Is the activity of the customer consistent with usual manner?

(i) Does the transaction or activity linked to the terrorist or terrorist group?

This list is not meant to be exhaustive.

8.6 Indicators of Suspicious Transaction/Activity

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

- application for business outside the policyholder’s normal pattern of business
- any want of information or delay in the provision of information to enable verification to be completed
- an atypical incidence of pre-payment of insurance premiums
- the client accepts very unfavorable conditions unrelated to his or her health or age
- the transaction involves use and payment of a performance bond resulting in a cross-border payment (wire transfers) = the first (or single) premium is paid from a bank account outside the country
- large fund flows through non-resident accounts with brokerage firms
- insurance policies with premiums that exceed the client’s apparent means

- the client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment
- insurance policies with values that appear to be inconsistent with the client's insurance needs
- the client conducts a transaction that results in a conspicuous increase of investment contributions
- any transaction involving an undisclosed party
- early termination of a product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party
- a transfer of the benefit of a product to an apparently unrelated third party
- a change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy)
- substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder
- requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments
- attempts to use a third party cheque to make a proposed purchase of a policy
- the applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract
- the applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments
- the applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency
- the applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify
- the applicant for insurance business appears to have policies with several institutions
- the applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means
- the applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party
- the applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy and

- the applicant for insurance business use a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

The above indicators are not exhaustive.

8.7 Employees and Agents Involvement in Money Laundering

- Changes in employee characteristics (e.g., lavish lifestyles or avoiding taking holidays).
- Changes in employee or agent performance (e.g., selling policy for cash, remarkable or unexpected increase sales volume).
- Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

8.8 New Customer/Policyholder

Although long-standing customers/policy holders may be laundering money through an investment business, it is more likely to be a new customer who may use one or more policy for a short period only and may use false names and fictitious companies. The following situations will usually give rise to the need for additional enquiries:

1. A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.
2. A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
3. A client with no discernible reason for using the firm's service; e.g., clients with distant addresses who could find the same service nearer their home base, or clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.
4. An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.
5. Any transaction in which the counterparty to the transaction is unknown.

8.9 "Tipping off" customer

The term "tipping off" simply refers disclosure of filing suspicious transaction/activity report to the customer. As per section 6 of the Money Laundering Prevention Act, 2009 any sort of tipping off is strictly prohibited. So, ICs must ensure the confidentiality of filing STR/SAR.

8.10 "Safe Harbor" provisions for reporting

MLPA, 2009 encourages financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. Section 28 of MLPA, 2009 provides the safe harbor for reporting. If the ICs fail to report STR/SAR they will be subject to punishment under section 25 (2) of MLPA, 2009

Chapter 9: Self-Assessment Process and Independent Testing Procedures

9.1 Self-Assessment Process

Each IC should establish an annual self-assessment process that will assess how effectively the IC's AML/CFT procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, who performed it, how it was controlled and supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of the IC have been properly discharged. The report should provide conclusions to three key questions:

- Is AML/CFT procedures in place?
- Is an AML/CFT procedure being adhered international requirement?
- Is an AML/CFT procedure complying with all policies, controls and statutory requirements?

9.2 System of Independent Testing Procedures

Testing is to be conducted at least annually by the IC's internal audit personnel, compliance department, or by an outside party such as the institution's external auditors. The tests include:

- interviews with employees handling customer/policy holder and interviews with their supervisors to determine their knowledge and compliance with the IC's AML/CFT procedures;
- a sampling of large transactions/policy followed by a review of transaction record retention forms and suspicious transaction referral forms;
- a test of the validity and reasonableness of any exemptions granted by the IC; and
- a test of the record keeping system according to the provisions of the MLPA and ATA.

Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken.

Annexure- A

Specific cases of money laundering

Life insurance

- On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank *accounts* and then transferred to an *account* in another jurisdiction. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas *accounts*. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

- Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean. To date, this investigation has identified that over USD 29 million was laundered through this scheme, of which over USD 9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.

- In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over USD 1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute.

  This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

- A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual‘s fraudulent management activity.

Non-life insurance

- A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.

- A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash installments. The insurance broker did not report the delivery of that amount and deposited the three installments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totaling USD 250,000, thus avoiding the raising suspicions with the insurance company.

- Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

- A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around USD 400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

Reinsurance

- An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

Assignment of claims

Non-life insurance – fraudulent claims

- Police in Country A uncovered a case of stolen car trafficking where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A. Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over USD 2.5 million. The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of damages.

  On receipt of the damages, the false claimants gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over USD 12,500 per month from the leader's accounts to the country in question. The money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its gains into real estate.

- An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that

would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honors the claim on the policy by paying off the loan on the vehicle. Thereafter, the organization running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of $2 million from similar fraud schemes carried out by terrorist groups.