Money Laundering and Terrorism Financing: Does the Saudi Arabian Financial Intelligence Unit Comply with International Standards?

Submitted in fulfilment of the requirements of the Master of Business by Research
(BRAL)

Abdulaziz Alhassan
Student ID: 3753359

Principal Supervisor: Dr. Edwin Tanner
Co-Supervisor: Mr. Abdul Rahman Mohamed Saleh

School of Law
Faculty of Business and Law
Victoria University, Melbourne

Nov 2011

ABSTRACT

Over the last decade, there has been an increase in the number of money laundering and terrorist financing crimes across the globe. In a bid for authorities to control these criminal activities both locally and internationally, the Financial Action Task Force (FATF) 40+9 Recommendations were established as a mechanism for identifying, combating and controlling money laundering activities. In compliance with Recommendation 26, each country should establish a Financial Intelligence Unit (FIU) to serve as a national centre for gathering, analysing and disseminating suspicious transactions related to money laundering and terrorism finance.

This aim of this research is to examine and investigate the compliance of the principle FIU within the Kingdom of Saudi Arabia (known as the Saudi Arabian Financial Unit) to the International Standards of combating money laundering and terrorism financing. This research also examines the effectiveness of SAFIU in dealing with prevention of money laundering and terrorism finance based on the 40+9 FATF Recommendations. Examining these aims is important as no previous research exclusively examines the compliance of SAFIU to the International Standards.

This study employed a survey-based research in the form of questionnaires completed by 74 civilian and uniformed SAFIU staff members. To assess the effectiveness, over 70 questions were provided to the respondents to acquire quantitative data for analysis purposes. Open-ended questions were also provided to accommodate opinions, comments and feedback.

Results showed that SAFIU was largely perceived as highly effective in receiving, analysing and disseminating suspicious transaction reports. It was also perceived to be effective in administering and coordinating activities with government and non-government institutions. Internationally, SAFIU was also perceived as being effective in cooperating with foreign FIUs through its Egmont Group membership. The study however identified a number of areas, such as training and development, where SAFIU was perceived to be less effective.

DECLARATION

I, Abdulaziz Al Hassan, declare that the Master by Research thesis titled 'Money Laundering and Terrorism Financing: Does the Saudi Arabian Financial Intelligence Unit Comply with International Standards?' is no more than 60,000 words in length, including quotations exclusive of tables, figures, appendices, bibliography, references and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work.

…….. …….

Abdulaziz Al Hassan Date

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

List of Tables

List of Figures

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering Law
AMLC	Anti-Money Laundering Council
AMLMAC	Anti-Money Laundering Law Monitor and Analysis Centre
AMLSCU	Anti-Money Laundering and Suspicious Cases Unit
ARIMA	Analysis and Auto-regressive, Integrated, Moving Average
AUSTRAC	Australian Transaction Reports and Analysis Centre
BDPC	Belgian Data Privacy Commission
BNM	Bank of Negara Malaysia
BSAAG	Bank Secrecy Act Advisory Group
CARIN	Camden Assets Recovery Inter-Agency Network
CFATF	Caribbean Financial Action Task Force
CTF	Combating Terrorist Financing
ECR	European Criminal Record
ESW	Egmont Secure Web
FATF	Financial Action Task Force
FEC	Financial Expertise Centre
FFMS	Federal Service for Financial Monitoring
FinCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions and Reports Analysis Centre
FIRS	Federal Inland Revenue Service
FIU	Financial Intelligence Unit
FMS	Financial Monitoring Service
FSA	Financial Service Agency
GCC	Gulf Cooperation Council
GPML	Global Programme against Money Laundering
IAIS	International Association of Insurance Supervisors
ICT	International Currency Transfer
IDW	Investigative Data Warehouse
IMF	International Monetary Fund
IMoLIN	International Money Laundering Information Network
IOSCO	International Organisation of Securities Commission
IVTS	Informal Value Transfer System
KSA	Kingdom of Saudi Arabia
MCMRI	Malaysian Capital Market Regulatory Institution
MENAFATF	Middle East North Africa Financial Action Task Force
MER	Mutual Evaluation Report
MLR	Money Laundering Regulation
MOCI	Ministry of Commerce and Industry
MOFA	Ministry of Foreign Affairs
MOI	Ministry of Interior
MOJ	Ministry of Justice
MOU	Memorandum of Understanding
MROS	Money Laundering Reporting Office Switzerland
NAATI	National Accreditation Authority for Translators and Interpreters
NCC	National Coordination Committee
NCIS	National Criminal Intelligence Service
NGOs	Non-Governmental Organisations
NTFIU	National Terrorist and Finance Intelligence Units
OECD	Organisation for Economic Cooperation and Development
OIC	Organization of Islamic Conference
PEPs	Politically Exposed Persons
POCA	Proceeds of Crimes Act
PCCML	Permanent Committee on Combating Money Laundering
PCCT	Permanent Committee on Combating Terrorism
PPO	Public Prosecution Office
SAFIU	Saudi Arabian Financial Intelligence Unit
SAMA	Saudi Arabian Monetary Agency
SAR	Suspicious Activity Report
SOCA	Serious Organised Crime Agency
STR	Suspicious Transactions Report

TFT	Terrorist Finance Team
UAE	United Arab Emirates
UIC	Ufficio Italiano dei Cambi
UK	United Kingdom
UN	United Nations
UNDCP	United Nations Drug Control Programme
UNSC	United Nations Security Council
USA	United States of America

CHAPTER 1: OVERVIEW OF THESIS

1.1. Introduction

The international community is undergoing rapid political, social and economic development. The use of modern technology has facilitated transportation and communications, and has made the world a small village. Although these developments have brought about positive outcomes globally, they have however, impacted the financial system exposing it to abuse from organised criminals. One of the major abuses of the world financial system is money laundering.

According to the 1998 Vienna Convention, money laundering involves the conversion or transfer of property, with the knowledge that that property is derived from an illegal activity, or from participation in such an illegal activity. The purpose of this activity is to disguise the illicit origin of the property, or to assist any individual who is engaged in such an activity to dodge any legal consequences of his or her actions (cited in Mitsilegas, 2003). Of late, money laundering has bee used to support terrorist activities. The World Bank cites financial terrorism as the 'financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism' (World Bank, 2009, p. 88). Money laundering and terrorism financing are closely related because the techniques used to launder money are practically similar to those employed in concealing the sources and applications of terrorist financing. This is a point supported by Schott (2006), who states that there is a close link between money laundering and terrorist financing, as the methods used in money laundering are similar to those used in concealing the sources of terrorist financing. Whether the source of terrorist finance is legitimate or illegitimate, terrorists conceal their sources thereby achieving continuity in financing and blocking detection.

The increase in the number of money laundering crimes is increasing, despite the growing efforts to stop it. These increases highlight the need to control such criminal activities at an international level through the sharing of intelligence between countries. Further, funds for terrorists raised from money laundering are also a big threat to global peace. As a result, the Kingdom of Saudi Arabia (KSA) has taken several measures to combat both crimes. The KSA has participated in many bilateral and regional agreements relating to combating money laundering and terrorism

financing. This includes the adoption of regulations set by the international financial advisories and other governing institutions (Cordesman & Obaid, 2005). In addition, in 1995 the Central Bank of Saudi Arabia (Saudi Arabian Monetary Agency – SAMA) established a national legislative, regulatory and supervisory framework for the banking and financial industry. This framework was designed to ensure that each financial institution remained vigilant, and that internal controls, processes and procedures were in place to monitor suspicious money laundering transactions and activities. Further, the KSA issued a Royal Decree under the Anti-Money Laundering Law (AML) in 2003. This Decree established a Saudi Arabian Financial Intelligence Unit (SAFIU) in the Ministry of Interior (MOI) which specialised in the handling of money laundering and terrorism finance cases (SAMA, 2008).

This thesis touches on the various sections of the KSA legal framework that deals with money laundering and terrorist financing. It also addresses how the KSA complies with international standards and agencies such as the Financial Action Task Force (FATF).

1.2. Problem statement and aims of study

The aim of this thesis is to investigate and examine the effectiveness of the principal agency in the KSA that deals with the prevention of money laundering and terrorism financing, the SAFIU. It will also investigate whether SAFIU complies with the international standards that have been set. Previous research has been conducted into money laundering and terrorist financing within the KSA - some focussing on the role of SAFIU, while others have concentrated on the effectiveness of security organs in combating the crime of money laundering.

Although these studies have been carried out, this particular research will focus on the effectiveness of SAFIU whilst evaluating the compliance between international standards and the KSA legal framework. Analysing the effectiveness is vital as the number of suspicious reports received by SAFIU since 2004 has increased significantly as indicated in Table 1 (MENAFATF, 2010).

Table 1: STRs from Reporting Entities 2004 – 2010

Year	Financial Institutions	Non-Financial Institutions	Government	Individuals	Total Reports
2004	341	-	5	4	350
2005	430	-	13	8	451
2006	316	14	14	61	405
2007	566	32	45	100	743
2008	787	28	133	71	1019
2009	956	11	215	48	1230
2010	1137	1	171	59	1368
Total	**4173**	**86**	**596**	**351**	5566

Source: MENAFATF, 2010, p.53

By examining the effectiveness of SAFIU, its policies and whether they comply with international standards, this thesis will also identify the challenges and issues faced. It will also focus on the Law Enforcement Model as this is the main model that is enforced within the KSA.

In summary, the key aims of this thesis are to:

1. Analyse the effectiveness of SAFIU in receiving and analysing money laundering reports
2. Analyse the effectiveness of SAFIU activities in administering money laundering activities in concert with other government and non-government agencies
3. Evaluate the relationship between SAFIU and the FIUs in other countries
4. Provide recommendations to SAFIU thereby enabling it to develop policies that better detect and combat money laundering and terrorism financing

1.3. Context of study

Many countries have policies that are designed to curtail the operations of money launderers. However, what is important is whether these policies are sufficient in attaining their intended objectives. Nations have attempted to develop counter measures that would limit financial crimes, if not prevent them. As a response to international AML regulations, the KSA has developed a number of initiatives, rules and laws to strengthen its legislative and regulatory framework nationally, regionally and internationally.

1.3.1. National efforts

The KSA has taken a number of measures designed to establish an institutional framework for combating money laundering and terrorism finance. In 1995, the government established a national specialized AML unit within SAMA. This unit obligated all the commercial banks operating in the KSA to establish an internal AML department to ensure that the banking system adhered to the international standards. During the same year, a committee known as the Permanent Committee on Combating Money Laundering (PCCML) was established. This committee was charged with the three main responsibilities:

- Coordinating AML and CTF policies
- Implementing FATF standards
- Heading the Saudi delegation to Middle East North Africa FATF (MENAFATF), FATF and other various international organisations.

The PCCML constitutes members from SAFIU, MOI, SAMA, Ministry of Justice (MOJ), Ministry of Commerce and Industry (MOCI), Ministry of Foreign Affairs (MOFA), Prosecution Authority (PA) and Saudi Customs. Further, a Permanent Committee on Combating Terrorism (PCCT) comprising of MOI, Ministry of Finance (MOF) and SAMA was constituted in 2001 to oversee and coordinate efforts to combat terrorism financing in the KSA (MENAFATF, 2010).

1.3.1.1.Towards financial institutions

In 1995, a framework for preventing money laundering and terrorist financing activities named ‘Rules Governing AML and CTF’ was issued by SAMA to all banks and money exchangers. This framework ensured that a customer’s identity, record keeping and suspicious transactions were reported to authorities. These rules were updated in May 2003 to further strengthen the implementation of ‘Know your Customer’ policies. As a result, non-residents were not permitted to open a bank account without the approval of SAMA. Further, SAMA also issued guidelines to all the banking institutions in the Kingdom to prohibit charities from transferring money overseas (Cordesman & Obaid, 2005). Alowain (2005) highlights that some of the prominent goals of this manual included:

- Assisting banks to comply with FATF recommendations

- Protecting financial institutions from money laundering and terrorist funding crimes
- Implementing laws and policies to eradicate money laundering and terrorism finance activities.

Other noteworthy initiatives that the KSA undertook include:

- Establishing an AML unit in 2001 at the Ministry of Commerce to provide guidelines and rules specific for commercial business (Cordesman & Obaid, 2005)
- Issuing the third update of the 'Rules Governing the Opening of Bank Accounts and General Operational Guidelines'
- Establishing an AML unit within the Security and Drug Control Department,
- Establishing AML and CTF Committees consisting of executives from various government agencies
- Implementing a declaration system for transporting cash equivalent to SAR 60,000 when entering or leaving Saudi Arabia
- Establishing a communication channel between MOI and SAMA to resolve issues related to terrorist financing (SAMA, 2008)
- Engaging the Nayef Arab University for Security Sciences to develop AML and CTF training programmes that were designed to educate judges, prosecutors, bankers, custom officers and other government agencies (Alowain, 2005).

1.3.1.2.Towards charity organisations

The 2003 Rules Governing AML and CTF were also extended across charitable organisations, requiring them to obtain a license to operate from the Ministry of Labour and Social Affairs and Ministry of Islamic Affairs. Some of the key elements of this framework for non-profit organisations include:

- Seeking authorisation from SAMA to open accounts for national or international charities
- Prohibiting the cashing of cheques issued in foreign currency
- Gaining authorisation to operate subsidiary accounts as charities are only to operate from a single account
- Prohibiting the use of credit or automatic teller machine cards for charity accounts
- Ensuring at least two individuals from the board of the charity are authorised to operate the main bank account

- Prohibiting the international transfer of funds from charity accounts (Cordesman & Obaid, 2005).

After the tragedy of September 11, a Saudi National Commission for Relief and Charity Work Abroad was established to manage and audit all the donations and contributions of charitable organisations operating within the KSA. This was in response to the nine additional recommendations developed by FATF (Cordesman, 2009).

1.3.2. Regional efforts

Within the region, the KSA has participated with fellow Arab nations in combating money laundering and terrorist financing crimes. The KSA for example has:

- Signed and ratified the Arab Anti-Terrorism Agreement in 1988
- Signed and ratified the Organization of Islamic Conference (OIC) Agreement for the Combating of International Terrorism in 1999
- Signed and ratified the Gulf Cooperation Council (GCC) for the Terrorism Security Agreement in 2004
- Become a member of the Middle East North Africa FATF (MENAFATF) (SAMA, 2004)
- Signed and ratified the Arab Agreement in preventing the Trade of Narcotics and Drugs in 1994
- Created the United Arabic Law in Drug Trade Prevention convened by the Council of Interior Ministers of Arab Countries in 1996
- Implemented a new strategy of law enforcement between the partner gulf countries in 2001
- Authenticated the Unified Law in 2001 to avert money laundering on behalf of Gulf Council (Alowain, 2005).

1.3.3. International efforts

Over the past decade, increased global efforts have been made to combat money laundering and terrorist financing. The KSA has taken several important efforts at the international level:

- Signing and ratifying the Vienna Agreement (The United Nations Convention on Illicit Traffic of Narcotic Drugs & Psychotropic Substances) in 1998
- Signing and ratifying the International Convention for the Suppression of the Financing of Terrorism in 1999

- Signing and ratifying the United Nations Convention against Transnational Organized Crime in 2000 (Alowain, 2005)
- Initiated multilateral agreements to combat money laundering and terrorism financing with countries from Asia, Europe and the USA (Cordesman, 2003a)
- Freezing Taliban financial assets and funds based on the UN Security Council Resolution 1267 in 1999
- Freezing funds of individuals based on UN Security Council Resolution 1333 in 2000
- Signing the International Convention for Suppression and Financing of Terrorism based on UN Security Council Resolution 1373 in 2001
- Acquiring membership of the GCC who collectively is a member of FATF (Cordesman, 2003b).

In 1988, the KSA joined with the UN to combat illicit trafficking of narcotics and psychotropic substances. Every quarter, the KSA submitted reports to UN detailing its initiatives and actions performed in their fight against terrorism. Through such efforts, the KSA requested Interpol arrest 750 people, of which 214 were of Saudi nationals believed to be involved in money laundering and terror financing activities (Cordesman, 2003a). The KSA also set up a real-time communication system between the MOI and SAMA to deal with matters relating to terrorist financing activities. Further, the KSA regularly participates in G-20 conferences and has implemented all the relevant recommendations issued by the G-20 forum in relation to terrorist financing (Cordesman, 2003b). Furthermore, the KSA completed the Mutual Evaluation Report by a team of FATF assessors based on the 40+**9** FATF Recommendations in September 2003 and was one of the first countries evaluated under this new methodology (SAMA, 2004).

These recommendations were developed by the intergovernmental organisation FATF. Initiated by members of the G8 countries in 1989 (France, the United States of America, the United Kingdom, Russia, Japan, Italy, Germany and Canada), FATF's responsibility is to develop international policies to combat money laundering and terrorism financing. One of these Recommendations is No.26, which states that countries are to establish an FIU that will monitor the trends of Suspicious Transactions Reports (STRs) and other information on money laundering or terrorist financing. The FIU should be able to access any financial, administrative and legal

information to achieve effective investigations (Zagaris, 2010). The United Nations (UN) Convention 2003 re-asserts this by maintaining that state parties establish an internal regulatory and supervisory body that will monitor, analyse, coordinate and prepare reports of suspicious financial transactions (UNODC, 2007).

Further, the capital city of Riyadh in Feb 2005 hosted the 'Counter Terrorism International Conference' aimed at highlighting the causes leading to terrorism and validating the relationship between money laundering and terrorist financing. The conference also enabled attendants to share experiences and solutions relating to terrorist group compositions and their operating patterns (MOFA, 2005).

1.3.4. The establishment of SAFIU

The SAFIU was established in the KSA in 2004 according to Article 11 of the Saudi AML Law, as stipulated by the Royal Decree No. M/39 dated 25/6/1424 H/24/8/2003 (see Appendix A). SAFIU is charged with the responsibility of receiving, analysing and preparing reports of all suspicious operations and transactions from all financial and non-financial organisations (MOI, 2007). FATF also recommended that each country should declare financing of terrorism as an offence punishable in law. Through the 'Rose Garden Strategy', countries are to freeze funds or assets belonging to those who finance terrorism (Ryder, 2011). Using such recommendations as a benchmark, the KSA has framed the AML Law policies in Article 16. These policies stipulate the measures that are to be implemented in order to curb money laundering and the punishment that is to be imposed on the perpetrators.

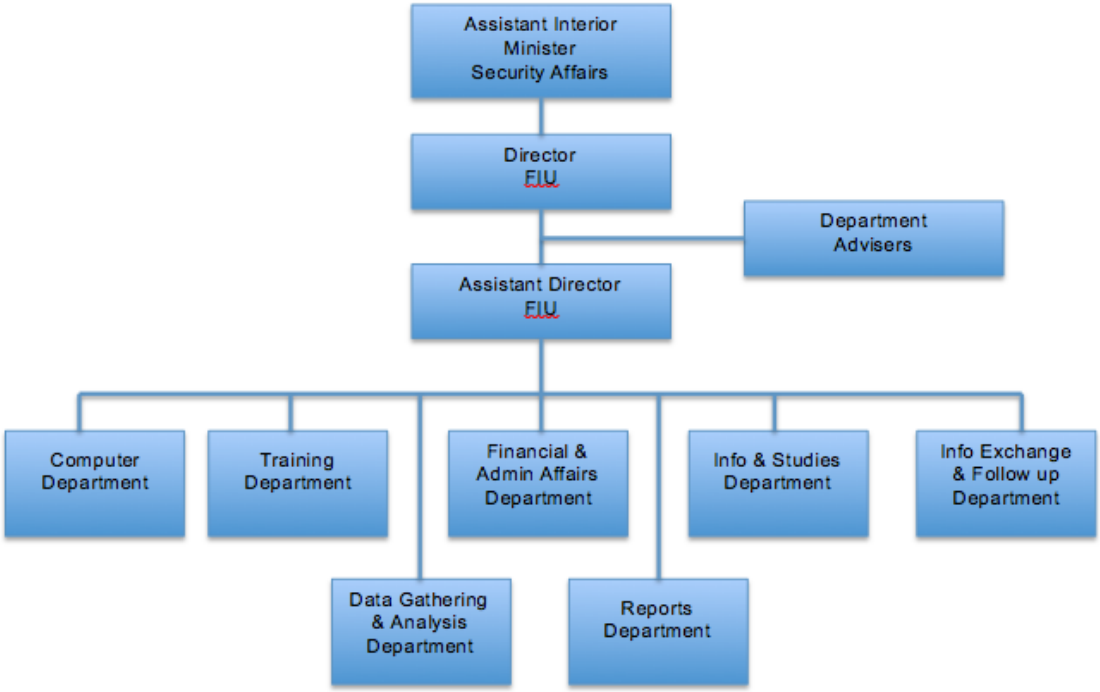
SAFIU has three core functions. Firstly, it receives Suspicious Transaction Reports (STRs) related to money laundering and terrorism financing. Secondly, SAFIU analyses these reports and identifies trends, patterns and other indicators of criminal activities. Thirdly, it disseminates analysed information by providing reports to law enforcement agencies and international bodies. SAFIU also performs additional functions, including conducting research, monitoring compliance and training the staff of reporting entities. Consisting of 111 staff members, SAFIU consists of seven divisions:

- Reports Division
- Information Collection and Analysis Division

- Information Exchange and Follow-up Division
- Information and Studies Division
- Training Division
- Financial and Administrative Division
- Information Technology Division.

Figure 1 details the current organisational structure within SAFIU (MOI, 2007).

Figure 1: SAFIU Organisational Structure



Source: MOI, 2007, p.7

1.4. Significance of the study

1.4.1. Academic contribution

This research provides an analysis of current AML practices in the KSA. Whilst there is no shortage of literature on money laundering, this thesis fills a void, as no previous research exclusively examines the compliance of SAFIU to the International Standards. By focusing on the effectiveness of SAFIU in fighting against money laundering and terrorist financing, this thesis provides a theoretical foundation that is designed to contribute to future research as academic review, analysis and evaluation of SAFIU's compliance and effectiveness towards International Standards is non-existent. In addition, the thesis nurtures and extends the existing academic framework of the Saudi Arabian Legislation by establishing the challenges faced by the country

in adapting to international standards. It is also hoped that this study will encourage similar studies, and as such, assist in making FIUs more robust.

1.4.2. Practical contribution

This study will make a practical contribution to SAFIU, government agencies, international organisations and academic researchers. In particular, the study:

1. Analyses the functions, roles and responsibilities of the SAFIU
2. Contributes to fellow researchers and academics by providing knowledge on the functions of SAFIU, and how this agency combats money laundering and terrorism finance
3. Evaluates whether the SAFIU complies with international standards
4. Identifies the effectiveness of SAFIU, and provides recommendations to address any weaknesses.

These practical contributions are to be extended to provide frameworks, mechanisms and methodologies that may be used collaboratively to improve broader regional cooperation in the KSA, Middle East and North Africa. This is important, as compliance mechanisms that assess whether FATF recommendations have been implemented should go beyond checking whether an FIU has been established. Such compliance is to include evaluations on the organisations management, operational policies, financing arrangements and skill development (Sathye & Patel, 2007).

1.5. Chapter summary

This chapter provided a general overview of money laundering, terrorism finance, the link between the two and the increasing need to curb these criminal activities. The aim and purpose of study was detailed prior to providing context on the national, regional and international efforts the KSA has implemented. A background to SAFIU was also provided prior to detailing the academic and practical contribution this thesis aims to impart. The next chapter (Chapter 2: Literature Review) will examine the existing literature to define and illustrate the functions of FIUs.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

In legal terms, organised crime involves a permanent association established to execute criminal activities through the application of means and techniques commonly agreed on. This is done with the aim to unlawfully obtain a high level of income and therefore constitutes a severe threat to order and public security (cited in Scherrer, 2009, p. 83). The key activities of organised crime revolve around its source of its income. Income is drawn from the provision of illicit means and the use of violence to procure money from legitimate businesses. A sizable portion of income for organised crime is derived from prostitution, narcotics distribution and loan sharking. Additional billions are also derived from theft rings, gambling, pornography and other illegal ventures (Siegel, 2008). As organised criminals are either directly or indirectly motivated to acquire financial gains illegally, there is an incentive for criminals to avoid detection by concealing unlawfully acquired funds. One mechanism used by organised criminals to conceal funds is money laundering.

2.2. Money laundering

The term money laundering is believed to have originated in the United States of America (USA) from Mafia groups who acquired substantial amounts of money from gambling, prostitution, extortion and bootleg liquor. Utilising laundromats as a mechanism of legitimising their funds, the Al Capone laundromats' are thought to have triggered money laundering as a method for legitimising the proceeds of crime. Lacey Lansky was The Mob's accountant, and is thought to have been one of the first, and perhaps the most influential, money launderer of his time. Utilising Swiss bank account facilities to integrate the first laundering techniques, Lansky applied the 'loan back' concept, which meant that illegitimate money could be concealed as loans provided by compliant banks from other countries (Duthel, 2008).

2.2.1. Definitions of money laundering

The act of money laundering is not a modern form of criminal activity, however the use of this term and its integration within the law enforcement paradigm is relatively new. According to Interpol (2011), money laundering involves an attempt to disguise or conceal the identity of proceeds obtained illegally in order to make them appear as

if they have been obtained from legal sources. This definition is accepted by the International Monetary Fund (IMF), which argues that 'money laundering is a process by which the illicit source of assets obtained or generated by criminal activity is concealed to obscure the link between funds and the original criminal activity' (IMF, 2011).

There is an agreement amongst academics as to the definition of the term money laundering. He (2010) for example, defines money laundering as a process whereby the source of dirty money is concealed to make it appear legal, and subsequently become usable, negotiable and transferable. Similarly, Duthel (2008) defines money laundering as what transpires when illegal money is concealed through a series of deals and transfers so that it appears legitimate. Hopton (2009) also states that money laundering is the process through which criminals disguise the origins of proceeds arising from criminal activities by converting dirty money to clean funds. Similar to Interpol's definition, Odeh (2010) defines money laundering as the process of accumulating the incomes of crime into the legitimate path of financial commerce by camouflaging its source and making illegitimate funds appear authentic.

Article 1 of the Saudi Arabian 2003 AML defines money laundering as 'committing or attempting to commit any act for the purpose of concealing or falsifying the true origin of funds acquired by means contrary to Shari'ah or law, thus making them appear as if they came from a legitimate source' (MOI, 2003, p. 2). Criminals apply different techniques of laundering money. Reuter and Truman (2004) cite cash smuggling, Hawala, insurance policies, casinos and securities as methods of money laundering. Thompson (cited in Griffith, 1997) on the other hand, points to bodies such as travel agencies, real estate, jewellery stores, shell-companies and credit unions as methods to launder money.

2.2.2. Stages of the money laundering process

The World Bank (2009) states that money laundering constitutes passing funds through three stages of *placement, layering,* and *integration*, with the aim of ensuring that funds appear clean at the end of the process. Placement, layering and integration are expressions applied by law enforcement agencies to define the three stages through which proceeds attributed to criminal activates are laundered. *Placement* is

the stage where the physical currency penetrates into the financial system and illegitimate proceeds are deposited in monetary establishments. In the *layering* stage, a launderer may carry out a sequence of financial transactions so as to develop a layer between the funds and their illegitimate source. This stage aims at concealing trails of evidence by creating numerous transaction layers to further disguise the funds from their original source. In the *integration* stage, illegitimate funds are incorporated with funds from legitimate sources as they gain access to the mainstream economy. Ways for possible re-entry of funds into financial institutions are through real estate purchases and shell company schemes therefore making it challenging to distinguish the legal funds from the illegal ones (Odeh, 2010).

2.3. Terrorism financing

Terrorist gangs often secure their funds through criminal activity even though their ultimate goal may not be economic gain (Forman, 2006). A terrorist organisation's key objective is to coerce a population or a government to carry out or refrain from carrying out a particular deed or action. To achieve these ends, terrorist groups need financial support and often operate in relative anonymity deploying unusual financing mechanisms like Informal Value Transfer Systems (IVTS) such as Hawala, cash couriers and the internet to store, move and earn assets through cohesive networks (Wesley, 2010).

2.3.1. Definitions of terrorism financing

It is worth noting that a significant number of conventions at the international level have been unable to consensually define a universal term for terrorism. To define terrorism globally is perplexingly difficult without taking into account the nature of the crime or method deployed. Definitions therefore vary, and are dependent upon particular frameworks based on the relevant body (Sorel, 2003). Article 2 of the 1999 UN International Convention for the Suppression of the Financing of Terrorism provides the following definition for terrorism financing:

> 'Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, 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 any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 any act.' (UN, 1999)

The IMF defines terrorism financing as the process through which individuals or organisations collect funds with the aim of applying those funds to the execution of terrorist deeds. This process has been outlined in the International Convention for the Suppression of Terrorism Financing and the annexes attached to it (IMF, 2003). This denotation is similar to the World Bank's (2009) definition which states that terrorism financing is any form of financial support towards terrorism, or those who conspire, participate, and encourage the execution of terrorist deeds.

2.3.2. Characteristics of terrorism financing

Terrorist financing can be applied as two distinct types of activity. Type 1 terrorist financing refers to the early stage of gathering large proportions of funds, while Type 2 terrorist financing refers to utilising the acquired funds to financially support a terrorist operation (Parkman & Peeling, 2007). By using a sophisticated method to move funds between jurisdictions, terrorists operate and monitor funds from a wide variety of sources around the globe. They utilise the skilled services of accountants, lawyers and bankers, and also exploit various products of financial services. Though the total funds required to manage the entire network is extraordinarily high, the funds involved to execute an individual attack may be quite small (Commonwealth Secretariat, 2006).

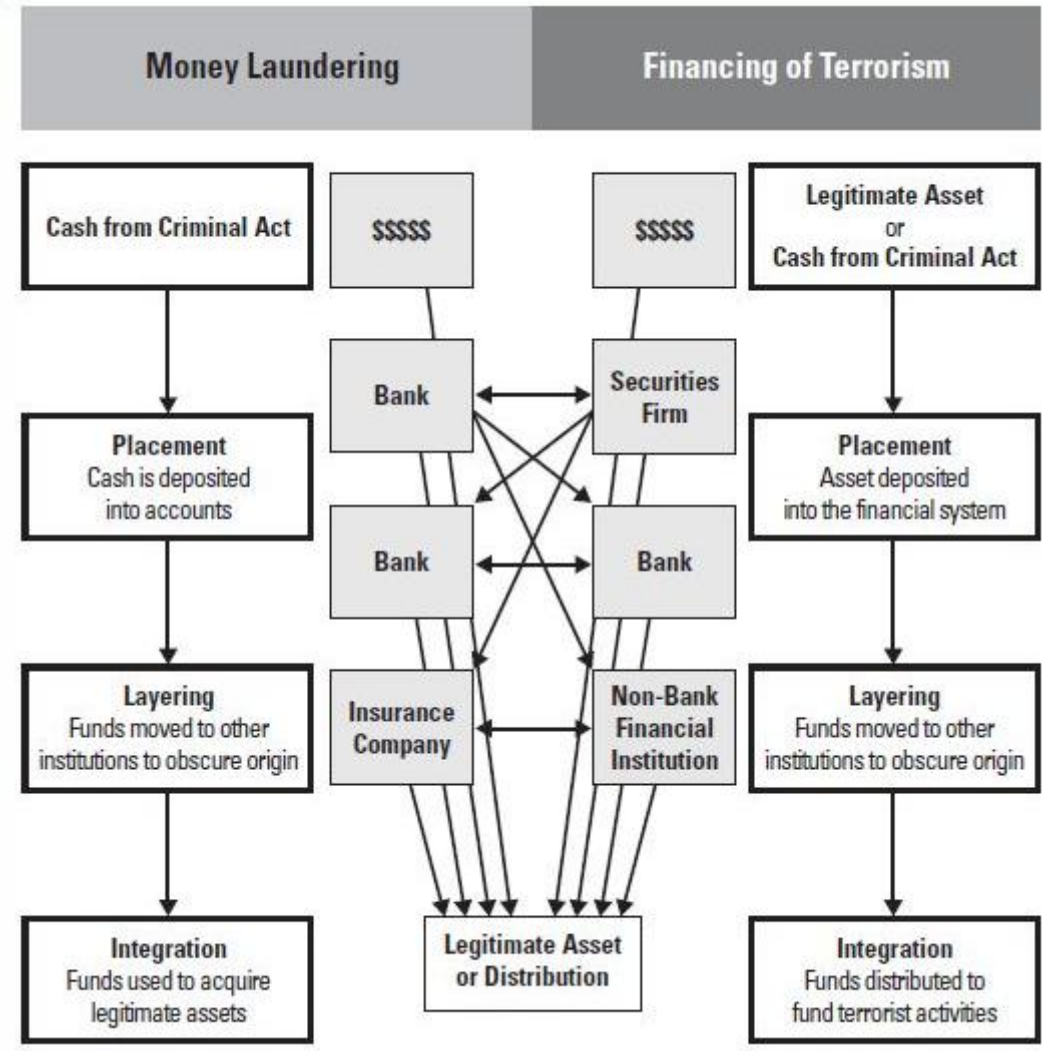
Criminal sources provide a consistent stream of revenue generated from human trafficking, kidnapping, extortion, drugs, gambling and smuggling. Although terrorists succeed in raising funds through illegal activities, transferring and laundering of such proceeds rely mainly on the methods followed by legitimate sources. This is primarily done to conceal the source of the funds and effectively transfer them to the preferred country. Some of the legitimate sources through which financial contributions are secured include charities, fundraisers and publications (Parkman & Peeling, 2007).

2.4. Links between money laundering and terrorism financing

The techniques applied in money laundering are synonymous with those applied in disguising the origins and uses of terrorist funds. Monies applied in funding terrorism may either be generated from criminal activities, legal sources, or both. However, it is necessary to conceal the origins of terrorism funding irrespective of whether the sources are legitimate or not. The implication is that if the source of funds can be disguised, then it would be difficult to prosecute terrorism acts. Additionally, it is imperative that terrorists and terrorism organisations disguise the origin of their funds so that the funding continues without being detected (Schott, 2006).

Money laundering and terrorism finance share a number of similar characteristics of combining monetary actions with criminal misdemeanour. Wesley (2010) asserts that similarities attributed to terrorism financing and money laundering lie in the procedures, tactics and techniques applied by both organisations when disguising and transferring funds. Similarities exist in the layering of the finances to disguise their origins and the ability to identify and take advantage of countries with weak legislations. As it is imperative for terrorist organisations to develop and maintain a concrete financial infrastructure, they utilise money laundering to facilitate their goals. However, the key difference between the money laundering and terrorism financing is that money laundering involves illegally obtained money, whereas terrorism financing entails both legitimate and illegitimate funds. Johnson (2008) similarly highlights that since the September 11 terrorist attacks, regulations of their financial systems in curbing money laundering were considered as an indispensable component of fighting the war against terrorism. Figure 2 elaborates on the processes and links between money laundering and terrorism finance (World Bank, 2004).

Figure 2: The Processes and Links of Money Laundering and Financing of Terrorism



Source: World Bank, 2004, p. I-8

2.5. Implications of money laundering and terrorism financing

Money laundering presents a number of implications for nations and their citizens. Economically, money laundering presents four main consequences: economic distortion, risk to financial institutions' integrity and reputation, government resources and socioeconomic repercussions. Economic distortion occurs because money launderers are usually not concerned about generating profits legitimately. Rather, their interest lies in protecting their proceeds and concealing their illegitimate origins. They may therefore invest their funds in ineffective activities that could culminate in high opportunity costs and impede economic growth. Money laundering also tarnishes the reputation of financial institutions. This may lead to job losses and culminate in other criminal activities that negatively affect economic development. In terms of

government resources, money laundering makes it difficult for governments to collect taxes and consequently reduces revenue, since most transactions occur within the underground economy. There are also socioeconomic repercussions in that if money laundering is not constrained, it amplifies criminal activities and leads to greater social ills. This in turn affects global market stability, destabilises commercial trades and increases explicit and implicit enforcement costs (Inter-American Development Bank, 2005). Additionally, Beare and Shneider (2007) highlight that money laundering increases the demand for cash, thereby affecting the stability of global markets and commercial trading as exchange rates become more unstable.

Money laundering also facilitates and amplifies corruption politically, where politicians and weak public officials in third world countries are encouraged to siphon public funds in return for kickbacks and bribes. In certain countries, these actions lead to political instability as laundered funds are utilised by individuals to achieve political ends (Ashford & Dauncey, 2006). In addition, money laundering also has social concomitants. These arise from escalating incidences of crime, bribery, corruption, contamination of legitimate businesses through illegitimate activities, and often result in dismantling of family units (Masciandaro et al., 2007). Money laundering enables criminals to expand their activities, and consequently increases government health, welfare and law enforcement costs. Coupled with corruption, the economic power possessed by money launderers spills over into every segment of the society. Schneider (2009) estimates the volume of money laundering in 20 Organisation for Economic Cooperation and Development (OECD) countries to be in the range of $515 billion to $614 billion during the period of 2004 to 2006.

Terrorism financing also has a profound impact on various aspects of humanity and economy. Funding of terrorist activities such as the September 11 attacks killed nearly 3050 people and inflicted damages close to $80 billion. Bali is another such example where a deadly explosion in a nightclub killed close to 200 people (Kunreuther et. al, 2003). Similarly, in March 2004, several bombs were detonated in commuter trains in Madrid killing 191 people instantly and injuring 1500 people (Beall, 2007). Such barbaric events indiscriminately inflict injuries and death against innocent civilians and cause widespread psychological, emotional and physical suffering among victims (Ashford & Dauncey, 2006). In addition, Frey, Luechinger and Stutzer (2007)

highlight that terrorism financing impacts a wide range of economic developments ranging from tourism, investments, stock markets, foreign trade and supply chains. Using a time-series analysis and auto-regressive, integrated, moving average (ARIMA) technique, the authors estimate losses in tourism revenue of around $16.145 billion due a high reduction of visitors choosing not to travel to European countries with high risk of terrorist attacks. Abadie and Gardeazabal (2008) also highlight that Foreign Direct Investment (FDI), a crucial source of government revenue and employment, can be considerably reduced in countries where terrorists attack thereby inhibiting economic growth and transfer of technical expertise into the country. Financial markets, such as the stock exchange, are also impacted as panicked investors choose to sell their shares at a rapid pace. This can increase inflation, cause recessions and lead to a higher unemployment rate (Drakos, 2004).

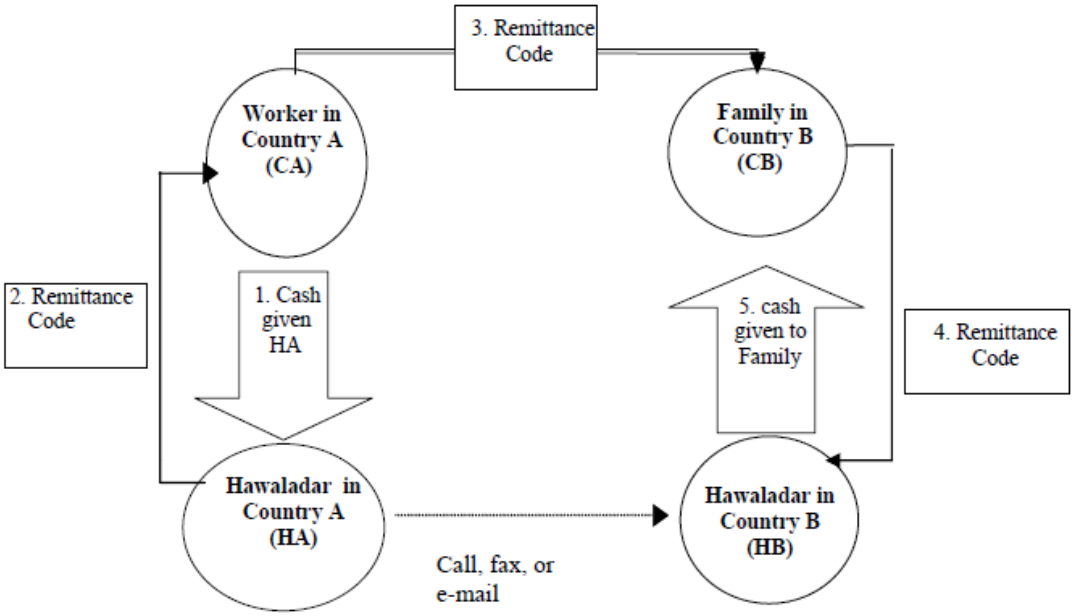
2.6. Case study: Hawala as an informal value transfer system

Hawala is a financial institution that has been established over a period of centuries against the backdrop of improper regulatory systems. The term Hawala can be traced back to India in the early 11th century, and is derived from the Arabic language meaning 'transfer'. Hawala is also known through other terminologies such as Hundi (India), Padala (Philippines), Hui Kuan (Hong Kong), and Fei Chien (China) where it was primarily developed to expedite trade between distant regions (Qorchi, Maimbo & Wilson, 2003). Jost and Sandhu (2000) define Hawala as money transfer without the money movement. This is a point supported by Shanmugham (2004), who highlights that the Hawala system allows money to be moved around the world without the physical or actual movement of funds, and offers financial services even to inaccessible and remote areas. In the recent years, Hawala has gained considerable interest not just because of its economic impact on the migrants in developed countries, but primarily due to the fight against money laundering and terrorist financing. At a time when AML is stringently implemented, the informal nature of Hawala is believed to be mysterious and a weak link in the battle against money laundering (Bunt, 2008). Though majority of Hawala is widespread in Middle East, Asia and Africa, it also has a large representation in Europe and North America, where the migrant communities in 2005 used Hawala to remit around $200 billion to their native countries (Razavy, 2005).

2.6.1. Characteristics of Hawala

Operating outside the jurisdiction of traditional financial and banking systems, Hawala has operated as an alternative to remittance systems by transferring money to the destination countries without the actual exchange of money. Operating from small stores or spaces, this mode of transfer has been very effective in developing countries such as India and Pakistan, which operate an ineffective system for financial supervision and regulation (Shanmugham, 2004).

Figure 3: Prototype of an Informal Hawala Transaction



Source: Qorchi, Maimbo & Wilson, 2003, p. 7

An example of a Hawala transaction is presented in Figure 3, where a worker in country A (CA) coordinates with hawaladar (HA) to organise a transfer to his home country by making a payment in the desired currency. The Hawala intercessor (HA) receives the money by charging a small handling fee, provides a remittance code to the client and communicates with his hawaladar counterpart (HB) in the destination country to arrange for a payment in the local currency to the beneficiary. This is accomplished on the condition that the recipient presents the same remittance code as evidence when receiving the funds (Qorchi, Maimbo & Wilson, 2003). As such, Hawala presents a system where individuals separated geographically can offer

money to each other without the actual physical movement of transferring funds (Viles, 2008).

2.6.2. Benefits and disadvantages of Hawala

Hawala is a preferred alternative to the financial systems of remittance because it offers convenience, efficiency, reliability and cost effectiveness. Viles (2008) for example highlights that migrant workers tend to favour Hawala due to lower overhead costs, minimal set of regulations, and the ability to operate in rural, remote and underdeveloped villages where facilities such as banks do not operate. Though Hawala is widespread in Middle East, Asia and Africa, it also has a large representation in Europe and North America, where the migrant communities in 2005 remitted around $200 billion to their native countries using Hawala (Razavy, 2005). Hawala is also preferred due to its relative cheapness as the commission charged is significantly lower than that charged by banks and other remittance firms (Parandeh, 2009). Further, in war-torn ravaged countries such as Somalia and Afghanistan, Hawala provides the only possible service for transferring money cheaply, conveniently and swiftly. Viles (2008) highlights that Hawala was popularly utilised in the December 2004 Tsunami where Tamil refugees in Sri Lanka regularly received funds. In addition, Hawala transfers are also swift and efficient as money is received in less than 24 hours (Razavy, 2005).

While it may seem that many utilise Hawala for genuine money transfers such as supporting their families, criminals have exploited these networks as a mechanism for money laundering, tax evasion, fraud and financing of terrorist activities. Gurule (2008) for example highlights that the absence of electronic, written records and lack of identification make Hawala an attractive option for transferring terrorist funds. Similarly, Viles (2008) points out that Hawala is often deemed an emerging factor for international terrorism, as it functions mainly on trust between operators who are bound by family or tribe affinity instead of government regulation. As such, Hawala is of particular concern as the sheer volume of funds flowing through the system, coupled with the lack of written records, makes it cumbersome for governments and law enforcement agencies to track audit trails for investigations (Shanmughan, 2004). Further, Qorchi, Maimbo and Wilson (2003) highlight that Hawala has repercussions on implementing financial and supervisory policies such as:

- Impacting economic statistics
- Influencing stock exchange operations
- Loss of revenue as hawaladars are not subject to any service or sales tax.

2.6.3. Hawala, money laundering and terrorism finance

FATF acknowledges the potential of Hawala to be used to launder money and identifiea that Hawala is a substantial process used by businesses of all magnitudes to send money back to owner's country with reliability and minimum paperwork. Funds move between individuals known as 'hawaladars' who collect money at one end of the process and distribute money at the other end (FATF, 2000).

Trehan (2002) points out that conventional money laundering, in conjunction with Hawala has the ultimate benefit of eliminating the paper trail of transactions involved. As a result, it becomes impossible to track and find evidence of the whole process. Physical movement of the money is considered vital in money laundering to facilitate its integration layer and place it legitimate businesses. This can be accomplished by Hawala during the transfer process. Hawaladars also benefit from using money laundering centres as remittance houses, and as central point for gold or silver smuggling.

Vaccani (2009) has indicated that alternate remittance systems such as Hawala are highly vulnerable to terrorist financing undertakings. The Hawala system has been employed to finance terrorist activities against Indian targets, with the main suspect is believed to have received RS 3.5 million via a Dubai based hawaladar. Funds were transferred in a similar fashion in order to carry out the November 2008 Mumbai attacks, where the suspect received money from a local hawaladar. On the other hand the 9/11 Commission did not possess any strong evidence about the use of Hawala systems by al-Qaida to finance attacks in US cities. However in the early stages of its operations, al-Qaida has successfully moved gold and cash from Afghanistan to Pakistan using hawaladars in both countries. Terrorist outfits seem to constantly monitor the government activities to adjust their strategies and in doing so there was an apparent shift from the formal banking systems to the informal systems i.e. Hawala (Vaccani, 2009).

2.7. The setters of International Standards in combating money laundering and terrorism finance

As money laundering and terrorism finance is a global issue, a number of international standards have been developed to curb its proliferation. These include adherence and conformance to FATF Recommendations, UN conventions, the Basel Committee, International Association of Insurance Supervisors, International Organisation of Securities Commissioner, and the Egmont Group (World Bank, 2009).

2.7.1. The United Nations

The UN has initiated and implemented a number of efforts aimed at combating money laundering and terrorism financing. A fundamental tenet of the organisation is that the United Nations Drug Control Programme (UNDCP) develops programs and provides legal assistance against money laundering (Commonwealth Secretariat, 2006). It has also devised a program called the Global Programme against Money Laundering (GPML). This program provides guidance for states to introduce legislation that develops policies, enhances global cooperation and raises public awareness (Odeh, 2010). Post the 9/11 event, one of the significant initiatives launched is the International Convention for the Suppression of Terrorism Financing. This has caused signatories to generate laws that criminalise the financing of terrorist activities (Smith, 2007).

2.7.2. The Basel Committee on Banking and Supervisors (BCBS)

The Basel Committee was constituted in 1974 by Central Bank governors of 10 countries: Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, Switzerland, UK and the USA. The BCBS is a joint committee of AML and CTF that integrates the International Association of Insurance Supervisors (IAIS) and International Organisation of Securities Commission (IOSCO). The committee's main role is to set standards for the insurance, banking and securities sector for combating money laundering and anti-financing of terrorist activities (The Joint Forum, 2003). In December 1988, BCBS issued the 'The Basel Principles' to prevent the usage of banking sector for money laundering activities (Hopton, 2009). The organisation also assesses and evaluates whether inconsistencies or gaps exist when new recommendations and approaches are being implemented. Further, it assesses groups

that are susceptible to money laundering practices and offers assistance in dealing with the identified vulnerable traits (Muller, Kalin & Goldsworth, 2007).

2.7.3. International Organisation of Securities Commissioners (IOSCO)

The IOSCO is an alliance of securities regulatory agencies that was founded in 1983, and adheres to three fundamental principles; reducing system risk, ensuring investors' protection and security, and warranting fairness, efficiency and justice among free markets. During the 1990s, the organisation focused on implementing rules for combating money laundering by initiating the 'Resolution of Money Laundering' (Koh, 2006). Legislation enforced is to be upheld by security regulators across the globe. Some of the major requirements include record keeping and the monitoring of procedures to detect suspicious money laundering activities in financial transactions (Diekman, 2008).

2.7.4. The International Association of Insurance Supervisors (IAIS)

Established in 1994 and amalgamated as a non-profit body under the US National Association of Insurance Commissioners, the IAIS has followed the footsteps of IOSCO and Basel Committee by framing a set of policies in 1997 to supervise the insurance industry (Herman, 2002). In 2002, the organisation issued AML publications tailored at informing insurance firms and its supervisors about popular money laundering methods utilised in the insurance industry (Reuter & Truman, 2004). In addition, the IAIS also sets international supervision standards for financial systems, promotes collaboration among insurance regulators, and ensures that insurance AML regulations and policies are complied with (Koh, 2006).

2.7.5. The FATF

In 1989, the G-7 Ministers issued an Economic Declaration addressing various issues regarding international monetary developments. In conjunction with this declaration, the leaders collectively approved the formation of the FATF to deal with money laundering. FATF was charged with the responsibility of coordinating various measures developed with an aim of countering money laundering both from a local and global platform. Consisting of 34 members, FATF is a distinct inter-governmental organisation that aims at creating and enhancing anti-money laundering policies at both national and international levels. The FATF secretariat is housed in the OECD

headquarters in Paris. Since its inception, the FATF has been working on ensuring that its recommendations are recognised as the global standards of AML and Combating Terrorist Financing (CTF). The work of FATF, covering over 170 territories, has had a major impact on global detection and deterrence of money laundering and terrorist financing (World Bank, 2009).

2.7.6. The FATF 40+9 Recommendations

In 1990, the FATF issued 40 Recommendations as measures for identifying, combating and controlling money laundering activities. The Recommendations addressed a broad range of topics, including the development of a regulatory framework that caters for a country's financial system. These non-binding Recommendations were generalised, and aimed at offering nations some flexibility in implementing their regulations in specific circumstances. Following the September 11 attacks in the USA, the FATF broadened its mandate to include provisions regarding terrorism financing. These provisions are subject to an extra nine special Recommendations, creating a total of 49 Recommendations commonly referred to as the FATF recommendations (Odeh, 2010) (see Appendix B).

In addition to these recommendations, the FATF has also issued guidance on money laundering to non-financial businesses and professions like lawyers. In 2002, FATF issued a consultation paper that outlined a range of options for stimulating AML measures. The paper proposed that some AML laws be extended to certain businesses and professions, such as lawyers, and encouraged governments to create a risk-based approach to counter money laundering and terrorist financing (McCann, 2006).

2.7.7. The Egmont Group

In 1995, an informal group comprising different FIUs was established at the Egmont Arenberg Palace in Brussels to facilitate international cooperation in the areas of information sharing, communication, expertise sharing and training coordination. During this meeting, information exchange principles to be applied by FIUs for money laundering offenses were developed and published (Leong, 2007). Over the years, the informal group has grown from 14 to 120 FIUs and is known as the Egmont Group. With its secretariat office in Toronto, Canada, the Egmont Group's goal is to provide a platform for the FIUs around the world to fight against money laundering,

terrorist financing and other financial crimes. The working groups of the Egmont Group, its committee and the secretariat, meet three times per year. The annual plenary and the meetings among the members of the Group serve the purpose of building trust and familiarity within the financial intelligence community (Sharman & Chaikin, 2009). To enhance sharing of information among the FIUs, the Egmont Group has developed a best practice information exchange manual, which provides guidance on the sharing of information whilst considering the confidentiality and privacy of the information being shared (GAO, 2006).

2.8. Establishing an FIU

One significant Recommendation is No.26, which states that FIUs should be established by all countries to serve as a national centre for gathering, analysing and disseminating STRs. In a timely fashion, the FIU should have direct and indirect access to the administrative, financial and law enforcement information that it needs to effectively carryout its functions. The creation of a centralised unit is a significant measure in combating money laundering, and as such is deemed as a critical element of the AML system (Commonwealth Secretariat, 2006).

After establishing an FIU, countries should also consider applying for membership at the Egmont Group. The Egmont Group is tasked with enhancing cooperation between FIUs and as such is referred to as the global FIU coordinator. Countries are to accept the Egmont Group statement of purpose and its principles for exchange of information between FIUs for cases related to money laundering. The Egmont Group defines an FIU as a central, national agency, charged with the responsibility of receiving, assessing and circulating financial intelligence disclosures to relevant authorities. The FATF expanded this definition further by stating that an FIU shall be charged with the responsibility of developing a repository of reported information, evaluating suspicious reports, and sharing financial intelligence. The FATF also has an overall requirement that every national authority should exchange information and collaborate with their national and international counterparts (Hopton, 2009).

2.9. Types or models of FIU

Though the FIU models vary from country to country, they are largely categorised under four types:

- *Administrative Model* – this model is made up of a structure that is under the supervision of an agency other than judicial or law enforcement authorities. This model either constitutes a detached agency placed under some form of supervision (autonomous) or entirely independent from any form of supervision (independent). Administrative FIUs are established within the Central Bank or in the MOF, or equivalent agency, and as such are not responsible for supervising the compliance of other financial institutions. Examples of countries that operate under this model include Belgium and Poland.
- *Law Enforcement Model* – this type of FIU is established with the powers of law enforcement and closely operates with law enforcement agencies such as a Financial Crimes Agency. This benefit of this type is that FIUs are able to draw and share their information, sources and expertise to create a faster response to money laundering cases. Examples of countries that have implemented this model are Germany, the UK and the KSA.
- *Judicial Model* - the judicial model of FIU is established under the judicial branch of the state or under the authority of the prosecutor. Luxemburg and the Mediterranean country of Cyprus function under this model.
- *Hybrid Model* – this model integrates different combinations of the other models to form a single FIU. Of importance and of much relevance within this context is that in certain FIUs staff members from law enforcement and regulatory units are seconded to work with the FIU while continuing to execute their original agencies' powers. Norway and Denmark are examples of countries that operate under this model (Thony, 1996,; Gelemerova, 2008).

2.10. Assessing an FIU for International Standards compliance

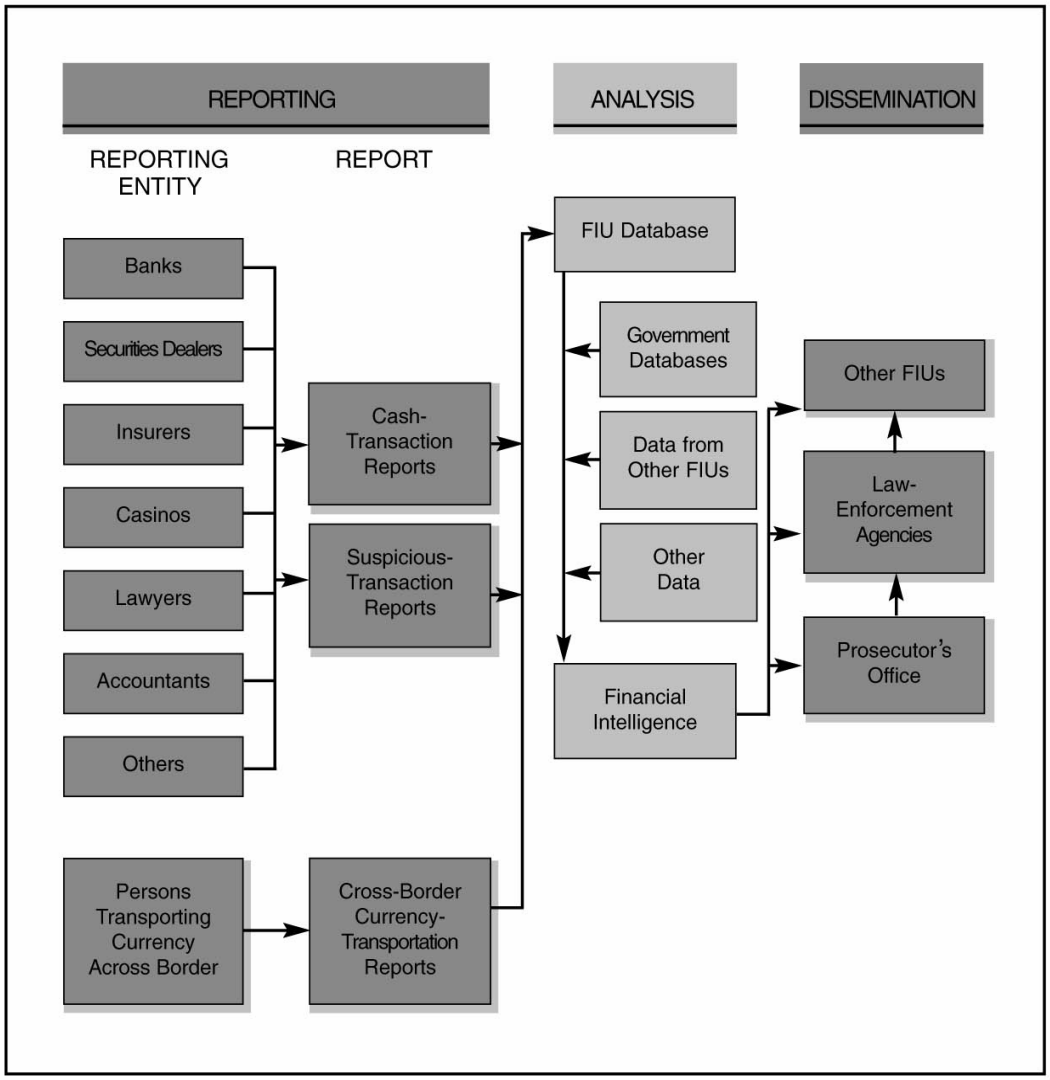
To curb money laundering and terrorism finance, it is vital for FIUs to be monitored and evaluated against international standards (Hopton, 2009). The FATF members played a leading role in setting the international standards and developed the FATF 40 + 9 Recommendations that in 2002 were endorsed by the Executive Boards of the IMF and the World Bank as the international standards against money laundering and terrorism financing (Kalin, Muller & Goldsworth, 2007). As such, it is mandatory for an FIU to be assessed on how effectively they have implemented the FATF 40+9 Recommendations. Due to the differing laws of sovereign states, Jensen and Png (2011) highlight that FATF has developed an assessment methodology to measure the compliancy rating of a country based on the implementation and management of the recommendations. Such assessments are to be conducted by FATF, IMF and World Bank once an FIU has accumulated statistical data spanning over four years.

Structural elements like governance, transparency and working culture have a significant impact on the effective implementation of an AML/CFT framework and are also considered by assessors who evaluate quantitative and qualitative data when assessing whether an FIU has implemented the recommendations. Other reports published by the UN, IMF and World Bank are also considered if they possess relevant information on the performance of an FIU.

2.11. Core functions of FIU

Although responsibilities of an FIU differ between countries, they share at least three basic core functions which include: receiving STRs, analysing STRs, disseminating reports for investigation and subsequent prosecution, and cooperating with other global FIUs and organisations (Schott, 2006). In addition to the core functions, FIUs also perform a number of supplementary functions such as monitoring compliance of policies and procedures, freezing accounts, maintaining databases and conducting training and awareness on AML and CTF issues. Figure 4 provides a high-level summary of a FIUs core functions (FINTRAC, 2001).

Figure 4: FIU Core Functions



Source: FINTRAC, 2001, p. Appendix III

2.11.1. Receiving reports

2.11.1.1. From financial and non-financial institutions

Financial and non-financial institutions are obligated by law to report suspicious transactions and other disclosures as dictated by a nations FIU unit (Odeh, 2010). This is to ensure that the FIU functions as a central repository that acquires, analyses and discloses information related to money laundering. Amassing information in a centralised repository creates more efficiency, which contributes to reduced money laundering activities both at a local level and globally. In addition, countries that practice the Law Enforcement Model are given additional powers including the power to conduct investigations that could lead to assets being seized or frozen. It is worth

noting though that FIUs are only able to exercise provisional powers concerning activities related to money laundering and terrorism financing (Gelemerova, 2008).

An example of the receiving report core function can be drawn from Sathye and Patel (2007). These authors carried out a study of Australia's FIU, which is a global pioneer. The study revealed that the Australian FIU, referred to as The Australian Transaction Reports and Analysis Centre (AUSTRAC), is legislated to receive money laundering and terrorist finance STRs from both financial and non-financial institutions. These institutions range from banks, credit unions, building societies, insurance intermediaries, dealers in securities, carriers of cash, trustees and managers of unit trusts and money orders. It addition, it also includes acquiring reports from entities who deal with travellers cheques, casinos, bullion dealers and currency remitters. The authors further indicate that the Indian FIU, (FIU_IND) perform identical functions to AUSTRAC in that they receive information relating to suspicious transactions from both financial and non-financial institutions. Though both FIUs are administrative types, differences exist in that AUSTRAC reports to the Attorney General's Department whilst FIU_IND reports to the MOF.

In Belgium, the Financial Information Processing Unit established by the 1993 Act has independent legality that grants it decision-making and budgetary autonomy. This unit has the authority to perform the functions of receiving, centralising and processing STRs from not only financial institutions but also from the police and other reporting agencies (Thony, 1996). In addition, the 1993 Act specifies that institutions are obligated to report money laundering and terrorism finance STRs to the FIU. Verhage (2009a) argues that this was not always the case as initially only financial institutions in Belgium were obligated to report suspicious transactions; however, non-financial institutions gradually espoused this AML legislation. This approach is also observed in Sweden where the FIU, National Criminal Intelligence Service, Financial Unit (NFIS) receives STRs from various sources such as banks, exchange offices, auditors, car dealers, casinos, money transfer agencies and financing companies as illustrated in Table 2 (Magnusson, 2009).

Table 2: Number of Money Laundering Reports from Various Sources in Sweden

Source	Number of Reports
Banks	1610
Insurance Companies	4
Exchange Offices	3815
Money Transfer Agencies	821
Financing Companies	3
Casinos	36
Car Dealers	5
Auditors	3
Real Estate Agents	1
Others	55
Total	***6353***

Source: Magnusson, 2009, p. 106

Switzerland was one of the first countries to criminalise money laundering through the 1997 Money Laundering Act. Under this Act, financial and non-financial institutions are under a legal obligation to report suspicious transactions to their FIU, the Money Laundering Reporting Office Switzerland (MROS). Institutions that fail to abide to the Act face a fine of 2 million Swiss Francs (Chaikin, 2009). In Italy, the law also states that all the financial bodies authorised to carry financial transactions must accumulate information about transactions that surpass a certain level and report to them to the Italian FIU, Ufficio Italiano dei Cambi (UIC) (Demetis & Angell, 2006). Japan also observes a legal obligation of reporting STRs to the Japanese Financial Intelligence Unit, JAFIO. The Financial Services Agency (FSA), being the regulatory body, monitors the compliance of financial institutions in accordance with AML and CTF regulations. To achieve this, JAFIO collaborates with FSA to improve their compliance (Kishima, 2004).

2.11.1.2. Fictitious companies

FIUs are also required to monitor financial transactions of fictitious companies and institutions, also known as ‘shell companies’ or ‘front companies’. A shell company is fictional, as it does not pursue legitimate operating activities. Criminals utilise such companies to conceal the illegitimate source of their funds. Front companies on the

other hand do exist, but are used for purposes synonymous to that of a shell company (He, 2010). The Egmont Group published a case study in which an individual established a fictitious car service station in a village to conceal funds that he had embezzled from his employer. His local bank reported a suspicious transaction to the FIU, which investigated the report and disseminated the results to the police for action (Egmont Group, n.d).

In another case study published by the Egmont Group, an individual in Europe had two accounts registered in the same bank. Funds originating from an offshore tax haven were deposited and immediately transferred to another account, leaving the original account dormant. This process was repeated on several occasions, triggering an enquiry which could not identify the source. Splitting the funds by transferring them to local companies initiated a series of investigation by the FIU about the individual and the companies. It turned out that these were fictitious companies and dummy corporations (Egmont Group, n.d).

Countries like Bermuda, the Bahamas and Virgin Islands have economic zones called 'offshore jurisdictional areas', which have reduced regulations. The concept is that investors who have their corporations registered in these jurisdictions do not need to visit the region personally, and are able to operate the business from any part of the world. When transferring funds, the financial institution is required to disclose the transfer to their corresponding FIU to obtain an approval to move funds. This process was implemented once it was exposed that there were serious financial frauds being committed using dummy corporations (He, 2010).

2.11.1.3. Other criminal activities

STRs received are not limited to the scope of money laundering. Article 4b of the UN Conference against Transnational Organised crime states that: Parties should aim to create FIU's to not only serve as national agencies for gathering, processing, and disseminating STRs inclined towards money laundering, but they should also serve as centres for probing into other financial crimes (cited in Mitsilegas, 1999, p. 157).

The United Kingdom (UK) FIU functions as a policing bureau as opposed to an administrative body, which is common in other countries. A policing structure was

implemented as the unit was taken over by the Serious Organised Crime Agency (SOCA). SOCA took over the responsibility of the FIU and its database from the National Criminal Intelligence Service (NCIS). It updated the existing infrastructure to enable agencies to access Suspicious Activity Reports (SARs) thereby clearing the backlog that existed whilst concurrently addressing the issue surrounding confidentiality (Leong, 2007). Currently, SOCA receives and reviews STRs that are related to other forms of crime in addition to money laundering and terrorism finance (cited in Preller, 2008, p. 236). A similar pattern is observed in Australia where the FIU is designed to receive low level intelligence that may be applied in probing potential criminal or tax offences. By contrast, the Swiss FIU focuses only on STRs related to money laundering and terrorism finance (Chaikin, 2009).

Another example can also be drawn from the USA's FIU, Financial Crimes Enforcement Network (FinCEN), which is charged with three key responsibilities: evaluating the financial intelligence concerning money laundering and terrorist financing received from financial intermediaries; implementing and controlling the Bank Secrecy Act; and overseeing the collection of global financial intelligence. In essence, FinCEN stems from the collection, classification and analysis of STRs (Bowers, 2009).

2.11.1.4. Reporting formats

As STRs are acquired from both financial and non-institutions, certain standards have been established when receiving reports. These involve; assessing the way a particular transaction was carried out; initiating proceedings related to the STR; alerting relevant authorities concerning the execution or the attempt to execute illegitimate transactions, and providing documents that indicate suspicious transactions to relevant authorities (Chlabicz & Filipkowski, 2001). Within SOCA, a common form is utilised by investigators to capture personal information and details of the crime from both financial and non-financial institutions. The institution that submits the report is to indicate the nature and reason for the suspicion, and provide additional information that allows the investigating officer to acquire a court order. SOCA is to acknowledge receipt of the form and appraise the reporting institution as to the investigation progress (Commonwealth Secretariat, 2006). Such investigations are initiated by the unit-reporting officer, whose responsibility is to monitor the whole process.

Substantial evidence is mandatory in such cases and absence of certain information will halt the investigation (Kalin, Muller & Goldsworth, 2007).

FIU_IND and AUSTRAC also provide institutions with a standardised form for submitting STRs. Though both countries provide standardised forms, differences in the format and cash limits requested exist. The Indian FIU for example has a threshold limit to receive reports of cash transactions above 1 million Rupees, (equivalent to roughly A$30,000) compared to A$10,000 in Australia. Sathye and Patel (2007) highlight that India's higher threshold is attributed to administrative causes, which indicate that a lower threshold would increase the pressure in processing suspicious transactions. FinCEN has also set a similar obligation to AUSTRAC where institutions are obliged to report cash transactions above US$10,000 to the US Treasury Department (He, 2005). Comparably, banks in Nigeria are expected to report transactions involving five million Naira for individuals and 10 million Naira for corporate transactions (Bolodeoku, 2009). Such limits contrast with Article 9 of the Swiss Money Laundering Act, which requires reports to be generated only for transactions of high substantial value (Chaikin, 2009).

Unlike FIUs in other countries, FIU_IND makes a distinction between financial and non-financial institutions, and as such provides a template for submission for STRs and Cash Transaction Reports (CTRs). This technique is also modelled by AUSTRAC, who provide reporting formats for bookmakers, solicitors, other professionals and non-business entities. In addition, templates acquired from banking institutions differ from non-banking institutions. However, forms which contain information related to STRs, International Currency Transfers (ICTs) and International Funds Transfer (IFTs) are identical (Sathye & Patel, 2007). Similarly, in Poland, STRs received undergo several processes that entail inter alia classification concerning the date and place where the transaction was exercised, the currency, amount and the nature of the STR (Chlabicz and Filipkowski, 2001). In Germany, the FIU developed a standard STR form to improve their reporting procedures in accordance with the AML Act. Ministers from the Department of Justice and Finance and state police department representatives reached an agreement on the form content based on the objectives set. Organisations and individuals utilise this form to

smoothen the reporting process by submitting STR to the relevant agencies and providing a copy to the German FIU (FIU Germany, 2004).

2.11.1.5. Receiving database

Concurrent with receiving reports, Demetis and Angell (2006) state that attempts by the FIU to profile or classify data is reliant upon the reliability of data sent from financial and non-financial entities. In effect, reliability of data is reliant upon information processes that inextricably become bound to the execution of profiling software and databases. This is a complex process, as receiving STRs is either impulsive or upon request, and achieved through various channels. In advanced Western countries like Australia and the USA, STRs are transmitted directly to the databases accessed by the FIU (Thony, 1996). In Germany, prosecuting authorities employ two distinct databases: the DOK Geldwasche and the FIU database, both of which are responsible for receiving incoming STRs (Preller, 2008). In the UK, the Elmer computer database, which contains information from financial, administrative and law enforcement units, is utilised to capture and store all the incoming SARs (Sproat, 2010).

As the UK FIU is under SOCA, it enables other areas such as the Terrorist Finance Team (TFT) and the National Terrorist and Finance Intelligence Units (NTFIU) to obtain additional information on identified suspects. This is because the SARs stored in the database not only provide basic information but other relevant data as well. Information stored in Elmer proved beneficial as 153 SARs were passed on to the NFTIU leading to the arrest of 24 individuals connected to a plot that was to explode a transatlantic airliner in 2006. Table 3 details the amount of information obtained and passed on to the TFT and the NTFIU database respectively (Sproat, 2010).

Table 3: Terrorist Finance SARs reported to UK FIU

Year	Terrorist Finance SARs	No. Passed to NTFIU
2002	4,775	512
2003	2,783	568
2004	2,248	672
2005	2,091	649
2006	2,089	907
2007		1,097
Oct 07 – Sep 08		957

Source: Sproat, 2010, p. 326-327.

In Germany however, the authorities who prosecute and the office that generates reports uses two different databases identified as DOK Geldwasche and the FIU database. This approach results in incomplete information as the number of SARs received by the prosecuting authorities and the FIU differ (Preller, 2008). Stefanou (2010) indicates that the European Union similarly lacks integration and cooperation of the various databases as the records held vary from one location to another. The advantage of having a centralised European database is that prosecutions and investigations become much easier and result in a better level of protection and accuracy. This is vitally important, as the digital revolution has presented opportunities for judicial and law enforcement agencies to develop collaborative databases that contain such information. These allow easy retrieval of information when investigations are pursued. Such an approach was evidenced in the USA, where the Investigative Data Warehouse (IDW), considered to be one of the most dynamic databases, is utilised to store information. IDW is centralised, web-enabled and provides information with a single query, making it possible to report significant information related to money laundering and terrorism finance (GAO, 2006).

In Canada, subsection 66(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing [PC (ML) TF] Act ensures that the Canadian FIU, Financial Transactions and Reports Analysis Centre (FINTRAC), is able to collect money

laundering information stored in databases preserved by other federal government agencies (Murphy, 2006). Similarly, the Chinese FIU in conjunction with other law enforcement agencies built a database consisting of high-risk customers by effective coordination and information exchange (Yan, Ai & Tang, 2011). Another example is also evident in the Nigerian FIU, where the database assists by disseminating its information with the Federal Inland Revenue Service (FIRS). By enforcing the applicable tax laws, FIRS utilise the information available within the database to combat corruption (Bolodeoku, 2009).

2.11.1.6. Privacy and confidentiality

A corollary of the obligation to report STRs requires that an individual who reports such transactions is to receive immunity from liability arising from reporting SARs (Gottselig & Underwood, 2004). In the event that information relating to money laundering and terrorist financing is disclosed, FATF Recommendation 14 (a) states that financial institutions, directors, officers and subordinate employees are to be protected from legal and contractual provisions that require an individual to disclose information even if they are unsure of the underlying criminal activity or whether the activity is considered to be illegal (cited in Shehu, 2010, p. 146). This point is supported by Chaikin (2009), who states that laws such as the Safe Harbor Law protects financial institutions and the employees from civil and criminal liability, thereby encouraging them to act without fear of retribution.

Section 25(A)(iii) of the 1994 Drug Trafficking Act in Hong Kong for example, provides protection to individuals who provide information relating to money laundering and terrorism funding. These protective laws however, are only relevant in situations where an individual has reported the suspicious transactions with no malicious intent (Sham, 2006). Similarly in the UK, the Proceeds of Crimes Act (POCA) has two specific safeguards with regards to disclosure orders. One of these safeguards is that individuals who offer information to SOCA are granted anonymity, and another is that the information they provide cannot be used against them in the event of criminal proceedings (Kennedy, 2007).

2.11.2. Analysing reports

The second aim of an FIU is to determine whether data reported provides an adequate basis to warrant further investigation prior to disseminating results to prosecuting authorities. This process involves analysing STRs to identify leads to possible crimes that will be utilised in the investigation and inquiry process. The initial point for any investigation is through the SAR, which would have been filed by an institution. Analysts search their FIU database to verify whether any relevant information reported from other sources such as intelligence, international FIU and law enforcement agencies is available. Publicly accessible information from commercial and government databases are also interrogated to identify links (FINTRAC, 2003).

Prior to investigating STRs received, FIUs verify their nature in an attempt to classify them. For instance in Belgium, the FIU received a total of 114,463 suspicious reports between 1993 and 2006. Subsequently, these reports were verified and classified into various categories that assisted in identifying whether the reports were attributed to the same suspect or transaction. As such, only 8,032 cases were sent to the prosecutor's office for further investigation (Verhage, 2009a). Within SOCA, analyses of STRs are classified into two categories. The first approach uses the 'follow the money' technique, in which in-depth investigations are conducted to track the location of funds. The second approach investigates the 'net worth' to identify all the properties owned by the suspect. Net worth investigations are more information intensive, as the investigator's aim is to analyse and detect a pattern by collating related but isolated facts (Kennedy, 2007).

The analysis phase involves the integration of data, logical reasoning and hypothesis development to define the similar set of data. Hypothesis testing is then implemented to accept or reject the concepts based on the scenarios. Once the analysis is complete, the dissemination of results is conducted (Sathye & Patel, 2007). Analysts are tasked to access and analyse data in financial transactions between individuals, organisations and businesses in a chronological order. The aim is to detect inconsistent or doubtful behavioural patterns (Pieth, Thelesklaf & Ivory, 2009). In addition, Ross and Hannan (2007) indicate that the uncertainty factor, also known as risk-based AML, must be taken in to consideration when analysing STRs. Risk-based AML is referred to as a

'tick box' style approach that is applied in order to focus on meeting the regulatory requirements. Yan, Ai & Tang (2011) cited China as one of the nations which has implemented a risk-based regulatory assessment as a measure to increase awareness and improve the performance of AML practices.

In the UK, analysts at SOCA review the Elmer databases to ascertain whether information from other sources such as law enforcement agencies, foreign FIUs, commercial and government databases exist. Applying the dots metaphor, the analysis of dots are assessed and connected to frame information in context with other relevant events and data. The information derived is subsequently applied in developing action plans (Kennedy, 2007). Such an approach is also evident in Germany where the legislation on AML is based primarily on the German Criminal Code (StGB, 1971), code of criminal procedures (StPP, 1950), the money laundering law (GGWG, 1993) and supplementary legislation like the Banking Act (KWG, 1961). These laws enable the reporting office to take the primary role in collating and analysing the STRs along with the duty of reporting the new information to the prosecuting authorities. The reporting office in addition assists by identifying new suspects (Preller, 2008).

In the UK, the inability to report or abide by FIU stipulations can serve as grounds for suspicion, leading to further time consuming and costly investigations. In mitigating the fear of being fined for non-compliance, financial institutions submit large volumes of STRs, which present a challenge during the analysis phases. One of the issues faced by financial institutions is the limited capacity for employees of financial institutions to scrutinise reports and perform 'know your customer' testing. UK STRs received in 2003 by the former intelligence unit; NCIS have extended 14,500 reports in 1999 to upward of 100,000 reports. With STRs increasing annually due to fear of non-compliance, there is potential for databases to be inundated with irrelevant information. This presents a situation where it is difficult for FIUs to trace money launderers. Further, the excessive reports received made assessing every STR problematic and difficult. As a result, STRs are now further categorised, prioritised and profiled prior to being disseminated to authorities. It is worth noting that categorisation of these transactions depends on the veracity of the data sent (Demetis & Angell, 2006).

The levels of coordination in the analysis phase between financial and security specialists vary from one country to another. Results from a survey conducted in Belgium indicate that effective coordination was observed between law enforcement units and compliance officers in France but not in Belgium. Despite the banking industry complying with regulations, survey respondents indicated that the lack of information exchange and coordination was attributed to the attitude towards law enforcement units. These units, when probing into money laundering incidences, have a tendency to treat banks like suspects as opposed to partners. Another factor contributing to a lack of coordination in Belgium is the inability of compliance officers to trade information with the banking sector. This is due to the prevalent confidentiality legislation that inhibits information exchange between individuals in the banking sector and other organisations. The survey however revealed that effective coordination between law enforcement units and compliance officers is amplified by a significant presence of former law enforcement agents who facilitate close productive relationships (Verhage, 2009a).

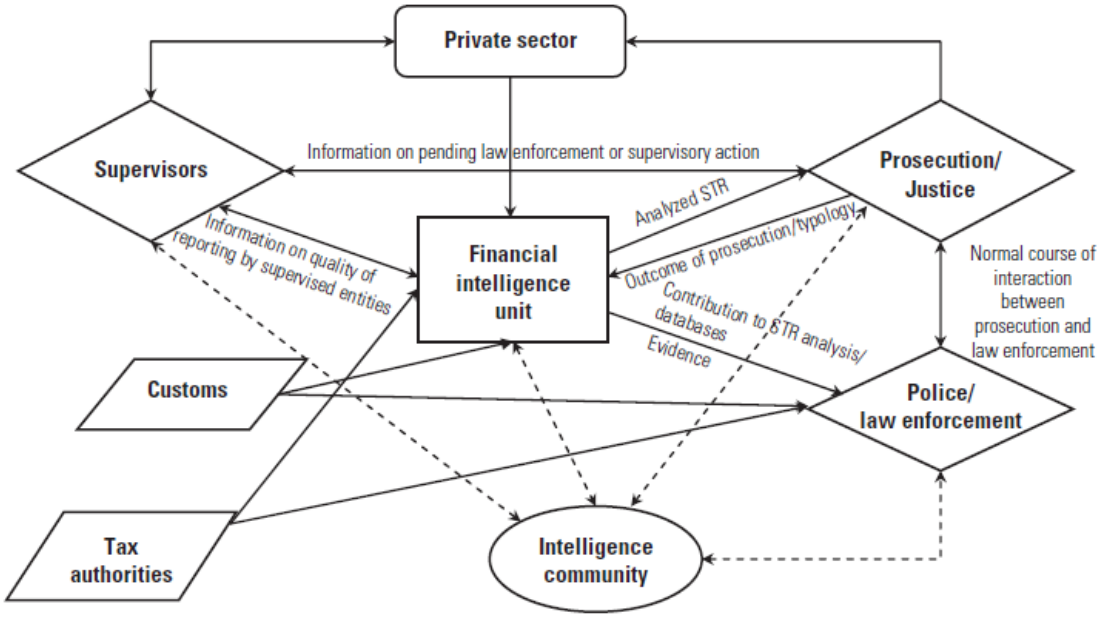
In Georgia, one of the measures utilised to measure efficiency of its FIU is through the number of investigations. These have risen from zero in May 2003 to 91 investigations over a three year period (Gotz & Jonsson, 2009). In comparison to the Italian FIU, the main feature is the absence of investigative competencies as the unit operates as an administrative type rather than an investigative agency (Biagioli, 2006).

2.11.3. Disseminating reports

The provision of FIUs to disseminate suspicious information to various government agencies is an integral part of any FIU system. In the global dialogue series published by the World Bank (2004), it states that FIUs are to ensure superior communication between law enforcement agencies and financial institutions. Further, FIUs are to develop mechanisms that constantly deliver feedback on STRs, thereby minimising legal constraints. This point is supported by the UK Commonwealth Secretariat (2006), who highlights the importance of frequently communicating feedback on the quality and volume of disclosures during investigations. In addition, information delivered frequently to the government departments, financial institutions and supervisory bodies improves efficiency and produces greater accountability. Ai,

Broome & Yan (2010) further highlight that the efficiency of AML and CTF rests on the willingness and ability to collaborate information exchange among financial organisations, FIUs, law enforcement agencies and international agencies. He (2010) elaborates further by stating that information exchange between police, customs and judicial entities improve capacity and capability in tracing suspicious transactions and illegal wealth flows. Figure 5 displays a framework where information sharing occurs between FIU's, law enforcement agencies, judicial and prosecution systems and other formal organisations (Chatain et al., 2009).

Figure 5: Domestic AML and CTF Cooperation



Source: Chatain et al., 2009, p. 150

2.11.3.1. Local cooperation

FIUs provide rules and regulations that outline the process of cooperation and coordination between government and non-government entities. Gottselig and Underwood (2004) highlight that the objective of any FIU is to decrease the number of offences involved in money laundering and terrorism finance ,and this can only be accomplished when all relevant agencies increase their individual effectiveness and cooperate with each other. Favarel-Garrigues, Godefroy and Lascoumes (2008) observed that a close cooperation and information exchange between police services and compliance officers in France benefitted the banking sector by exposing individuals engaged in money laundering activities early. The benefits of close

cooperation have also been realised in China where measures such as establishing the AML Monitor and Analysis Centre (AMLMAC) have strengthened the FIUs resources to work closely through the exchange of intelligence information related to money laundering (Sham, 2006).

Diekman (1999) stresses that it is essential for financial and security personnel to coordinate money laundering investigations. Security personnel have the skillsets of the anti-corruption agencies, ombudsman and audit department, whilst financial personnel participate in analysing financial information. Collectively, they serve as watchdogs that analyse STRs effectively. Similarly, Subbotina (2008) also observed that FIUs that cooperate with other agencies during the investigation phase demonstrate greater efficiency and better outcomes. The Russian FIU, Federal Service for Financial Monitoring (FFMS) for instance, coordinates with the Central Bank of Russia by defining the attributes and levies on the institutions failing to adhere to AML regulations. As such, the cooperation increases the efficiency of the investigations being carried out.

In Malaysia, the Central Bank of Malaysia (Bank Negara Malaysia) in conjunction with the Malaysian government have implemented AML legislation that incorporates information sharing and cooperation with other law enforcement units. Each agency is charged with certain responsibilities that are aligned to the FIUs goals. The customs and police department is charged with the responsibility of identifying the companies involved in money laundering. The Bar Council requires lawyers to report any form of suspicious transactions that are not consistent with a customer's profile. Non-Governmental Organisations (NGOs) apply similar rules that regulate non-profit companies and charities. NGOs in Malaysia are controlled and supervised by the Registrar of Societies who instruct organisations to submit their financial statements every year. If suspicious or unlawful transactions are detected, the FIU is notified (Shanmugam & Thanasegaran, 2008).

One of the notable measures in the Malaysian approach include the establishment of the National Coordination Committee (NCC) to combat money laundering, which was formed in April 2000. Chaired by BNM, the NCC is made up of representatives from 13 ministries and law enforcement bureaus that monitor and report on significant

money laundering and terrorist funding incidences. Representatives of the various Malaysian ministries that make up the NCC coordinate their concerted efforts by convening several times annually to report on their development and progress of outstanding issues and decisions (Shanmugam & Thanasegaran, 2008).

A similar joint approach is also evident in the America's, Europe and Asia. The Bank Secrecy Act Advisory Group (BSAAG) in USA constitutes the FinCEN, the Department of Treasury and Justice and various law enforcement agencies. This group receives reports from agencies and advises treasury on how to enhance the capability of departments to facilitate reporting efficiency. In the Netherlands, a Financial Expertise Centre (FEC) has also been established within the justice and finance ministries to combat financial crimes and safeguard the integrity of its financial system. FEC is part of the collaborative effort in which prosecutions, supervision, intelligence and criminal investigations are handled in unison (Chatain et al. 2009). In Hong Kong similarly, money laundering incidences are probed by the Customs and Excise Department in conjunction with the Hong Kong police. An outcome was that the reports are effectively passed on to the relevant investigative units such as the Customs Drug Investigation Agency affiliated to the Customs and Excise Department or the Narcotics Agency (Sham, 2006). Ireland has extended this approach further by developing a multi-agency approach where each team member holds rights and powers of access from his parent body thereby ensuring speedy retrieval of information. This Kennedy (2007) argues is one of the important reasons as to why the bureau is operating effectively.

As the information received by FIUs passes through several stages before being disseminated to fellow agencies, evidence indicates that certain FIUs do not promptly circulate the latest information pertaining to cases. This is apparent in countries where FIUs receive a large proportion of information that has to be verified and analysed on a first-come basis to ascertain its credibility. Prioritisation of STRs does occur especially in environments where analysing reported data is excessive for the FIU staff to efficiently manage (Demetis & Angell, 2006). In Russia, banks adhere to strict internal control rules, reporting, customer identification and record keeping set by the AML legislation (Subbotina, 2008). This has led to banks in China and Russia filing a

large number of STRs with the FIU, consequently overwhelming the unit and limiting its ability to analyse and disseminate reports effectively (Tang & Ai, 2010).

Further, certain countries indicate that there is a limit to the number of prosecutions conducted relative to the number of reports received. Demetis and Angell (2006) highlight that FIUs and courts are very limited in their capacity to investigate and prosecute every AML case, especially in countries where the number of cases has increased by up to six times. The authors evidence this principle to AUSTRAC where, in 2005, out of almost 11 million reports received only 1,743 led to investigations representing a meagre 0.016 per cent all reports received. This is also evident in the UK where technology and automation has intensified the process and created difficulties in coping with the increased volume (cited in Demetis & Angell, 2006, p. 168).

2.11.3.2. International cooperation

Within the international context, global organisations such as the World Bank and IMF have provided a platform for sharing information, developing approaches to common issues and promoting standards and financial policies specific to AML and CTF issues. In addition, these organisations have contributed to various FATF's efforts and have conducted assessments in the financial sector, performed research and undertaken training and awareness programmes, such as the distance learning network, mentoring programs and global dialogue (Leong, 2007).

Stefanou (2010) suggests a solution for developing a centralised database at the international level where information gathered is utilised in the prosecution of crimes committed across different countries. He (2010) follows a similar theme, which argues that the monitoring centre for AML should increase information exchange measures with their counterparts in different countries to prevent launderers from exploiting jurisdictions. Between 2003 and 2004, the Caribbean FATF (CFATF) held a convention in Antigua and Barbuda. The Chairman, Sir Ronald Sanders, called for a meeting to ascertain whether it would be possible to have regular forums for FIUs so as to enhance regional cooperation and share concerns about problems and issues. What emerged was a general consensus in favour of a regular forum backed by heads of member states' FIUs. Since this initiative was introduced, attendance at scheduled

forums, meetings, conferences and seminars has been exceptional, with a minimum of 25 FIU heads in attendance during each session. The initiative continues to progress positively, culminating into a success story for the region in signing collaborative agreements (Wilson & Rattray, 2007)

In addition to meetings, CFATF has developed a joint approach working with the South American FATF and the USA. The joint group is aimed at addressing the AML and CTF weaknesses concerning the transfer of money. Participants from the global community are invited to participate in sharing knowledge, expertise and enhancing global cooperation with an aim to establish a uniform structure for regulating the systems of global trade (Wilson & Rattray, 2007). Similarly in Malaysia, the FIU at BNM ensures that local efforts to counter money laundering are integrated with regional initiatives. They do this by conforming to the recommendations attributed to the OECD and cooperating with over 12 foreign and domestic bureaus involved in AML and CTF activities. Through such conformity, BNM has signed a Memorandum of Understanding (MOU) with the FIUs of a number of countries such as Indonesia, Australia, USA and the UK (Shanmugam & Thanasegaran, 2008).

Since 1995, the USA FIU FinCEN has focused its global efforts towards assisting jurisdictions establish new FIUs and improve their existing units. The number of FIUs increased from 14 in 1995 to 101 by the year 2006. This is a significant increase and was partly due to the training and technical support provided by FinCEN (GAO, 2006). FinCEN performs various activities, such as assessing other FIUs, providing advice on FIU legislation and presenting seminars on how to combat money laundering. It also specialises in training FIU personnel and provides technical advice on computer systems. In addition, FinCEN also exchanges personnel with foreign FIUs in order to acquire and share experiences as was seen during a personnel exchange with the Egmont Group allies from Baltic nations, Bolivia, Turkey, South Korea, Ukraine and Russia. In 2005, FinCEN provided training to FIUs in Argentina, China, Brazil, Paraguay, Sri Lanka, South Korea and Guatemala. In addition, a team of four was sent to the KSA in 2006 to provide presentations and conduct an on-site assessment of SAFIU. Further, by sponsoring South Africa, Bahrain and Mauritius as members of the Egmont Group, FinCEN assisted South Africa and Mauritius to become the first two countries in Africa to be represented in the group (GAO, 2006).

Germany's collaboration in the international stage is also noteworthy. Out of 606 cases investigated in 2004, the German FIU, Zentralstelle Für Verdachtsanzeigen submitted 504 requests to foreign FIUs and responded to 104 external requests. Though most of the requested information was related to fraud, narcotics and forgery, Germany played a crucial role in combating terrorist financing by assessing, supplementing and forwarding relevant information to overseas partner countries (FIU Germany, 2004).

In order to facilitate information exchange and develop collaborative programs, FIUs regularly hold meetings with each other to implement AML procedures. The FIUs in the Caribbean nations for instance regularly hold meetings to ensure that each participating country fulfils its responsibilities and discharge its duties efficiently. Meetings of such a nature provide an opportunity to assess the money laundering framework of partner nations and implement lessons learnt based on the experiences of other countries. These networks also act as a platform to deliver training and education programmes to help develop FIUs in overcoming operational challenges and deficiencies. In addition, such forums also create awareness about the recent trends in money laundering activities (Wilson & Rattray, 2007).

The Egmont Group has its own secure internet system called *Egmont Secure Web*, which enables members to communicate case information, post new technical developments and use analytical tools to assess information on typologies (Jensen, 2006). Maintained by FinCEN, the Egmont Secure Web provides FIUs with general analytical information and the relevant laws and regulations. Within this portal, FIUs are authorised to communicate within this secured network. Access to the Egmont Secure Web is endorsed by the statement of purpose and is accessible by the FIUs affiliated to the group. This restriction ensures that all the FIUs affiliated to the site have a shared responsibility in managing the information available within the site or exchanged via email (Mitsilegas, 1999). Kishima (2004) highlights that since JAFIO became a member of Egmont Group in May 2001, it has contributed towards the framework for information exchange internationally with foreign counterparts such as the British and Belgian FIU.

In addition to the Egmont's group statement, the AML unit of Interpol has forged alliances with different FIUs and crime units around the world to increase the flow of information amongst FIUs. Interpol's global police communication system, *I-24/7*, assists investigators around the world to cross check the data containing information on suspected terrorists, fingerprints, stolen identity documents and DNA profiles within seconds (Interpol, 2010). In 2000, another secured decentralised computer network called *FIU.NET* was established by the FIUs in the European Union. Serving a similar purpose to the Egmont Secure Web, France, Italy, Luxembourg, Netherlands and the UK initiated this model which became operational in 2002. By 2010, 24 of the 27 European Union member countries were connected to each other via *FIU.NET* with the remaining countries in the process of getting connected (Fiu.net, 2010). In 2006, the working groups of the Egmont Group met in Cairo to discuss the benefits of integrating both the secure communication networks, *FIU.NET* and *Egmont Secure Web*. The integration of the databases was approved and the migration of the Egmont Secure Web was completed in December 2006 thus enabling both networks to exchange information (Jensen, 2006). In addition, the European Union has developed an informal system that improves the effectiveness of the cooperation between the different FIUs. Camden Assets Recovery Inter-Agency Network (CARIN) is an international network utilised for tracing, confiscating and freezing criminal proceeds. Further, CARIN assists in identifying the national liaison officers who share information related to AML and CTF (Interpol, 2010).

Commercial companies are also utilised by financial institutions to provide information on suspicious transactions. This is due to the fact that databases utilised by FIUs vary from country to country and bank resources are not always available to provide expertise on AML information. Commercial companies are hired to provide software access to databases that contain information about convictions or frauds related to Politically Exposed Persons (PEPs), companies and individuals. These companies also issue reports, which not only provide information, but incorporate expertise and analysis that assist bank staff when conducting investigations. World-Check is an example of such a database (Verhage, 2009b). Lastly, information is also exchanged globally through the International Money Laundering Information Network (IMoLIN). IMoLIN is an internet-based network that provides access to the latest money laundering news and information (Diekman, 1999).

2.11.3.3. Annual reporting

In addition, FIUs regularly release periodic reports that contain statistics, typologies and trends, as well as information pertaining to its operational activities. In the Canadian 2003-2004 annual report, FINTRAC revealed that it had received more than nine million STRs, of which 160 were progressed to prosecution (cited in Murphy, 2006, p. 430). Similarly, the Nigerian FIU reported that it received more than 6700 STRs in the first half of 2008, of which 46 were subsequently developed into legal cases (NFIU, 2008).

2.11.4. Other Functions

2.11.4.1. As an authoritative and regulatory body

Chatain et al. (2009) state that as an alternative to the bank supervisory model, supervision of AML and CTF compliance can be conducted by FIUs. This model however requires banks to authorise access to all appropriate information, thereby enabling the FIU to regulate and monitor the institutions compliance to AML and CTF obligations. Implementing this framework offers a number of benefits, in that the FIU has direct simultaneous access to the databases of financial institutions and law enforcement authorities, thereby ensuring that STRs are analysed effectively (Murphy, 2006).

While the organisational structure of supervision varies from country to country, the FIU has provisions to guarantee independence and special grants of authority. Some of the best practices followed in many countries include:

- Adopting a risk-based or a standardised approach for compliance issues
- Being granted the freedom to be effective and not subject to external influences from other agencies
- Being accountable and governed to fulfil their responsibilities efficiently by building trust between public and private sectors
- Being granted powers to access information to monitor bank's compliance in STR filing and reporting
- Being given the authority to develop rules and impose relevant sanctions to regulate compliance and issue guidance
- Implementing off-site and on-site supervision for banking systems

- Being provided with sufficient financial and technical resources (Chatain et al., 2009).

Though monitoring generally falls within the domain of banking authorities, FIUs in countries such as the USA and Australia are empowered by law to monitor financial institutions. Whilst assessing the adequacy of legislative backing in context of a better functioning AML organisation, FATF commended AUSTRAC for adopting soft and effective AML practices (Sathye & Patel, 2007).

In Belgium, the compliance function is outlined in the AML responsibilities expected from financial institutions. The compliance department assumes the role of initiating and coordinating the financial institution's regulation. A compliance officer affiliated to the compliance department is not only expected to implement AML procedures but is also to carry out other tasks that ensure compliance. Some of the duties of a financial compliance officer include formulating guidelines for financial institution employees, developing code of ethics and procedures, training and amplifying awareness, auditing transactions, probing into rule violations, and following up on legislative requirements. As such, compliance officers act as AML gatekeepers and constitute processing the STRs from the reporting phase to the final phase of court hearings (Verhage, 2009a).

In the UK, SARs are made accessible to legal and prosecuting authorities. SOCA has authoritative and investigative powers that enable them to obtain information from financial institutions, and allow monitoring of real-time data in an account for every 20 minutes, for up to 90 days (Sproat, 2010). Further, the Money Laundering Regulation (MLR), which came into force in 1994, imposed several regulations on financial institutions and reporting entities. Regulations enforced covered procedures for record keeping, identity evidence and transactions, reporting and training employees on the process of identifying and reporting suspicious transactions (Leong, 2007).

Similarly in Nepal, the FIU is authorised to access and investigate transaction details of financial institutions, government entities and non-financial institutions (Sapkota, 2010). This is in contrast to the Zentralstelle Für Verdachtsanzeigen, which only acts

as a policing agency that ensures smooth integration between prosecution and regulatory bodies (Preller, 2008). FINTRAC also provides a relevant example within this context, as it does not have the authority or power to request additional information from its reporting institutions. Rather, it gathers reports, carries out its own analysis, and establishes whether it should disseminate the information to enforcement agencies (Murphy, 2006).

In addition, FIUs impose control on financial institutions to ensure they comply with policies relating to money laundering and terrorism finance. In the USA, convictions linked to money laundering extend to include non-complying institutions. Surveys carried out in both Belgium and France reveal that the perception of risk linked to non-reporting is significantly high with concomitant legal repercussions associated with non-conformity (Verhage, 2009a).

The Malaysian Capital Market Regulatory Institution (MCMRI) penalises directors and chief executive officer who utilise their senior positions to advance their own personal gains. Section 130 of the 1965 Companies Act disqualifies directors and CEOs convicted of aiding money laundering activities through dishonesty and fraud offences. Further, Section 100 of the Securities Act gives the Council authority to take pre-emptive action against any director who is likely to breach such laws (Shanmugam & Thanasegaran, 2008). It should be noted that the level of autonomy granted to an FIU varies from country to country. In Italy for instance, the FIU is constituted within the Central Bank, and as such receives autonomy and independence through a special statutory regime (Merlonghi, 2010).

2.11.4.2. Maintaining security and confidentiality

In conjunction with the provisions of member states, the European Union's legislation on data protection is strict on the collection, content, access and application of data attributed to money laundering and organised crime. Whilst assessing the development of the European Criminal Record (ECR), Stefanou (2010) established that the data stored in the European Union database is subject to protection laws and exemptions based on directive 95/46 of the ECR.

When filing an STR with the FIU, a confidentiality recommendation developed by FATF and endorsed by the IMF and World Bank is used. FATF Recommendation 14(b) states that financial institutions and their staff members are legally prohibited to reveal to clients that an STR has been initiated and reported. The requirement is to keep the information on the STR confidential from the clients or to any third party. In July 2005, the UN Security Council passed Resolution 1617, which requested its members to implement this recommendation (Chaikin, 2009). In Luxembourg, the FIU - Service Anti-Blanchiment, is located within the Public Prosecution Office (PPO), and as such adopts the mixed model approach of judiciary and the policing aspects. As STRs are generated at the PPO, Article 4 of the 1995 regulation empowers the PPO to set up and run a data bank on suspicious transactions, specifying that the information processed and recorded is to be accessed only by authorised members of the PPO (Mitsilegas, 1999).

Though financial organisations are assured of legal protection when filing reports, Ajayi and Abdulkareem (2010) argue that the contractual duty of confidentiality between the client and the bank is affected when there is an obligation on the part of the financial institution to report any suspicious transaction. Verdugo-Yepes (2008) discusses a confidentiality incident with the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a private organisation created in 1973 to handle the exchange of financial information. In this case, the USA treasury department utilised this program to secretly track terrorist financing activities. This led to the Belgian Data Privacy Commission (BDPC) criticising that SWIFT had not complied with European and Belgian data protection principles. Certain countries, such as Ireland, provide judges in the high court with the power to request information related to Trusts. In comparison to Australia, the Crime Commission Board acts an as overseer when requesting documents to be provided for court cases (Kennedy, 2007).

2.11.4.3. Accessing and maintaining databases

Advances in technology have enabled databases to monitor money laundering and terrorism finance related information. In addition, technology has also made it easier to link and transfer information between databases. Shared databases are of great assistance to investigators especially when recovering information about assets,

operations and suspects (Kennedy, 2007). Countries such as Australia and the USA utilise databases that are powerful and interlinked to police, customs, tax, company registers, electronic directories and newspapers. Information passed onto the FIU databases is transmitted electronically in the form of bank reports (Thony, 1996). Such benefits have been recognised by other countries such as China, which has required law enforcement agencies to develop a database that includes the names of all criminals involved in money laundering activities (Yan, Ai & Tang, 2011).

Murphy (2006) points out that in the event that FIUs need to make enquiries about money laundering and terrorism finance, they have the authority to access other databases that may have indirect or no access to. Some of these databases include administrative, public, law enforcement and commercial databases. A typical example is drawn from FINTRAC's pursuant to Section 54, which gathers information it deems relevant to money laundering and terrorist funding. FINTRAC has access to databases owned by provincial governments, as well as commercially available databases, enabling it to gather significant information (Murphy, 2006). Section 24c of the 1961 German Banking Act stipulates that banks and financial intermediaries be obliged to create customer databases that contain names, dates, account numbers, addresses and birth dates. The German financial supervisory authority has the authority to access such databases (Preller, 2008). Accessing information is also evident in SAFIU, where the agency has been empowered to have direct access to all government databases (MENAFATF, 2010).

2.11.4.4. AML, CTF training and qualified staff

Recommendation 15 of the FATF recommendations states that financial institutions are required to develop programs targeted against money laundering and terrorism finance. Such programs should include; signing up compliance and control officers, developing on-going staff training programmes, and implementing reporting standards that incorporate when, how and who to report to (Shehu, 2010). The World Bank (2004) also states that it is a requirement for law enforcement, public and private entities to be educated about case studies which illustrate real time complexities involved in AML and CTF. Specifically, staff and supervisors at all levels of financial institutions are to undertake training that provides a thorough understanding of the AML and CTF topologies and their precautionary measures and

laws. The IMF (2004) further highlights that for suspected transactions that are linked to terrorism finance, employees must be trained to ensure reporting entities detect the transactions which appear normal but are actually intended for illicit objectives. Such expertise enables STRs to be classified according to the appropriate crime.

Training programs are evident in Malaysia where FIU employees attend courses, carry out AML and CTF awareness campaigns, acquire skills in transaction analysis and formulate policies attributed to money laundering and forensic accounting. Staff are also trained in investigating asset forfeiture and other criminal matters (Shanmugam & Thanasegaran, 2008). Sapkota (2010) also highlights that such training activities occur in Nepal, where the FIU carries out workshops and training programmes that involve both government and non-government organisations. In addition, the Nepal FIU has carried out a series of interactive programs aimed at policy makers, bank chiefs and parliamentarians. These programs work towards creating awareness about the issue of money laundering and terrorism finance. Gotz and Jonsson (2009) also indicate that the Georgian FIU, the Financial Monitoring Service (FMS) has implemented a number of regulations that create better awareness of money laundering activities among its law enforcement agencies. It received 43,053 reports between Jan 2004 and April 2006, of which 1,313 were categorised as suspicious. The Nigerian FIU on the other hand was established at the beginning of 2006 and received only one STR in the first 18 months. This turned out to be a report sent by error (Sharman & Chaikin, 2009).

Within the KSA, the MENAFATF (2010) identified that non-financial institutions were not able to differentiate between the stipulated requirements of monitoring and reporting suspicious transactions. SAFIU was able to address these issues through a combination of training and increased clarification of rules and regulations. Guidance was also provided to supervisors, enabling them to provide training and guidance to their staff members. Similarly, AUSTRAC in its 2004-05 report has indicated several measures for up- skilling staff members by publishing a handbook that details performance management, development and job evaluations (AUSTRAC, 2005). AUSTRAC has also developed an e-learning application for cash dealers to access and acquire information and knowledge (Broom, 2005). Kennedy (2007) indicated that training seminars targeted to improve their capacity and skills in tackling

investigations efficiently were also provided at SOCA. In the case of the United Arab Emirates (UAE), the IMF (2008) highlights the nation's achievement in organising 360 seminars that enhance the performance and skills of various domestic and international FIU employees during 2004-08.

Supervisors who have knowledge in receiving reports also play a significant role. The First Mutual Evaluation Report (MER) published by FATF for China revealed that their FIU did not have precise requirements to assign a proficient compliance officer at management level to communicate STRs knowledge to employees. As such, the China FIU, Joint Financial Intelligence Unit (JFIU) designating a senior trained supervisor to ensure their staff members were capable of accessing STRs in a timely fashion. Such measures are vital as skilled supervisory staff are an essential part of the AML process which ensures that STRs receive the required scrutiny and rigour (Ai, Broome & Yan, 2010).

Whereas Insurance and Banking supervisors seek information on supervision and licensing concerning regulated institutions, FIU supervisors seek information linked to enforcement action against suspicious customers. The implication is that this enables the FIU supervisor to be aware of reputational risks and legalities that arise during money laundering and terrorism financing activities (Verdugo-Yepes, 2008). Chinese authorities also published a set of AML strategic development guidelines, which mandate a series of initiatives that indicate that China is supporting its AML framework. The guidelines include a system to develop a financial intelligence network that captures suspicious transactions in the sector of finance, government, banking, and non-banking institutions (cited in Ai, Broome and Yan, 2010, p. 394).

In the UK, the national policing plan 2004/07 identified access and privacy management skills as one of the eight core skills that law enforcement organisations and investigators are required to possess when recovering assets (Kennedy, 2007). In the Philippines, licensed partners for mobile banking have to undertake FIU training in AML and CTF policies. Similarly in South Africa, agents providing Mobile Phone Financial Services (m-FS) service must be trained and certified in AML and CFT by their FIU, the Financial Intelligence Centre (FIC) (Chatain et al., 2008).

FIUs are not the only entities investing in AML training. A survey conducted by the accounting firm KPMG highlights that banks have developed a strong preference towards training staff about transaction monitoring, thus making it the second biggest contributing factor to increased training costs (cited in Shanmughan & Thanasegaran, 2008, p. 339). Such outcomes were not evident in Nigeria, where a key concern as highlighted in the annual 2007 report indicated that the Nigerian banks failed to provide continuous AML and CTF training to their staff (cited in Ajayi & Abdulkareem, 2010, p. 39). Such training plays a vital role, as financial institutions are required to develop AML and CFT programmes that incorporate investigative, compliance and audit training. Developing awareness is vital, as FATF requires financial institutions to undertake special considerations when transacting with countries that do not apply FATF recommendations sufficiently. Iran is one such country (Chaikin, 2009).

In certain countries, the head of the FIU is appointed in the same manner as the civil servants of comparable ranks. In Brazil and Colombia, the President nominates the head of the FIU. In Bulgaria, the head of FIU is appointed by the Finance Minister who requires approval from the Prime Minister (IMF, 2004). FIU directors in countries like India and Australia are appointed by Ministers who are also empowered to remove them. AUSTRAC recruits its own staff from the public whereas the FIU_IND hires its staff from other government departments and the Reserve Bank of India. In addition, staff in FIUs are composed of experts from the police, finance, supervisory authorities and custom departments (Sathye & Patel, 2007). Economists, bankers, engineers and insurance specialists are also hired as experts who analyse reports. Background checks are conducted before hiring, as security is paramount to FIUs (IMF, 2004).

The proportion of staff accessible to an FIU is also of significant importance. Magnusson (2009) highlights that FIUs have to address problems arising from the large volumes of information received from STRs. Sweden in particular has a small number of only 20 officials who handle all types of reports. Staffing issues were also identified in the UK where prior to SOCA taking over, the NTFIU had 80 staff and nine contractors working on AML and CTF disclosures. Recommendations were considered by SOCA and staff levels were increased to 200 in 2006-07 with a staffing

budget of over £6 million (Sproat, 2007). In addition to a shortage of skilled staff and resources, Shehu (2010) indicates that West African FIUs are overwhelmed with an avalanche of impractical information that cannot benefit the implementation, investigation or prosecution of money laundering and terrorism financing activities. A similar outcome was deduced in FIU_IND, which was reported as having 43 staff in the year 2005. This value is notably low when compared to AUSTRAC, who in the same year had a total of 132 personnel forming around 36 per cent of the total annual budget of A$22 million (Sathye & Patel, 2007). A severe staff shortage across all member nations was a key item highlighted by the IMF during the annual plenary meeting of the Egmont Group in July 2005 (GAO, 2006).

With respect to SAFIU, its current resourcing level is 121, of which 20 positions are vacant and yet to be recruited to. In tandem with its annual budget of SAR 100 million, the agency is considered to be well resourced, however the effectiveness of staff members in handling and processing STRs effectively is an area that requires attention (MENAFATF, 2010).

2.11.4.5. Freezing accounts

The UN 1373 Resolution is a binding document that requires all member states to immediately freeze funds, economic resources or assets of persons who carry out, attempt to carry out, facilitate, control or participate in terrorist deeds (Leong, 2007). Currently, the Malaysian FIU, Unit Perisikan Kewangan, and Bank Negara Malaysia (UPWBNM) has authority to identify and subsequently freeze funds and assets attributed to terrorism (Shanmugam & Thanasegaran, 2008). Similarly in Zimbabwe, the FIU director has special powers to freeze accounts that are suspected of money laundering (Gubbay, 2007). Such authority is also evident in the Philippines where the Anti-Money Laundering Council (AMLC) can pass a motion to freeze property for a period of up to 20 days after pursuing civil forfeiture on cases that evidence unlawful activities (Simser, 2006).

Supported by Security Act of 2001, CTF policies in the UK also allow for forfeiture and seizure of suspect's financial assets. These policies have been strengthened more recently with the 2008 Counter Terrorism Act, which empowers the treasury to freeze assets and prevent financial support to specific persons or organisations that evidence

terrorism finance. Investigations carried by SOCA resulted in the freezing of 237 accounts suspected of financing terrorism (Sproat, 2010). In addition, Demetis and Angell (2006) estimate confiscations in the UK to be in the vicinity of around £46 million of criminally obtained assets. In Germany, a special analysis framework known as SPITAL, was established to investigate money laundering, corruption and misappropriation of funds by high-ranking government officials. Results published demonstrated that large numbers of suspicious accounts were evident leading to over €1.72 million being frozen in Germany and three other European countries (FIU Germany, 2004).

Similarly, assets investigated in Switzerland are quite substantial with STRs totalling 8.741 billion Swiss Francs. Though some of these funds were frozen, it is unclear exactly how much. STRs contributed to significant investigations pertaining to key personalities, such as Sani Abacha, the deceased Nigerian Dictator, Vladimir Montesinos, the former chief of Peruvian Intelligence and the former Prime Minister of Ukraine, Pavlo Lazarenko. In the cases of Sani Abacha and Montesinos, the Swiss authorities repatriated millions of dollars back to their respective countries (Chaikin, 2009). In Belgium, 8,032 STRs led to 939 convictions leading to prison sentences and asset seizures (Verhage, 2009a). Contradictory to this approach of freezing accounts, Magnusson (2009) indicates that Swedish bank regulations have large deficiencies that do not permit banks to freeze money related to suspicious transactions. In addition, independent companies in Sweden that handle currency and cash exchanges continue to remain anonymous to the FIU.

2.12. Chapter summary

This chapter examined existing literature to define and illustrate the FIUs functions. The background and implications of money laundering were considered prior to discussing terrorism finance and the characteristics that link these criminal activities. The international standards attributed to combating money laundering and terrorism finance were described to provide context. FATF recommendations were then introduced to explore the process and demonstrate the types of FIUs that exist. The focus then shifted to discussing the core functions of FIUs, where evidence from different nations was presented to elaborate FIU roles in receiving STRs from financial, non-financial and fictitious institutions; analysing reports and disseminating

STRs locally and internationally. Other functions, such as the FIU's role in acting as a regulatory body, maintaining confidentiality, training staff and freezing accounts were also examined. In the next chapter (Chapter 3: Methodology) the questions, design of study and scope are illustrated. The chapter also details the data collection methodology and presents the strategies that will be utilised for analysing the data.

CHAPTER 3: METHODOLOGY

3.1. Introduction

This chapter presents the methodological approaches used in this study. These areas are highlighted through the study's focus in analysing whether SAFIU complies to the International Standards set. The following sections provide an explanation and justification of the chosen research design. Demographic information of the respondents is then provided prior to presenting the data collection method of constructing, validating and translating the research instrument. An outline of the pilot study and the analytical procedures utilised during testing are also detailed.

3.2. Research design

The research design employed in this study is survey-based in the form of questionnaires. The survey method was deemed as the most appropriate research design for this thesis as the researcher was able to collect quantitative data needed to identify the effectiveness of SAFIU. Though the study predominantly employed quantitative methodology, a number of open-ended questions were also provided to accommodate information that is difficult to quantify, such as reasons, opinions and comments. This type of information was left unaltered in order to maintain its value (Johnson & Christensen, 2007).

Quantitative research was employed in order to categorise the answers from the respondents to the survey questionnaire, and also to analyse the results through a statistical approach. On the other hand, the qualitative research was accommodated to assess the non-quantifiable answers of the respondents in terms of their experiences and opinions regarding the subject matter. In addition, the use of related references and primary documents was also considered in this study as a qualitative type of research. Qualitative information, especially those based on the personal experiences, can provide a greater insight and in turn present a more in-depth understanding of the subject at hand. This methodology is thought to be the most appropriate for this research because it diversifies all the aspects of the data collection and assists in gaining a more thorough understanding of the subject matter (Johnson & Christensen, 2007).

3.3. Ethics approval

The research instruments were approved by the Victoria University Human Research Ethics Committee (VUHREC) under the reference number HRETH 10/233 on 2 December 2010. The instruments of this study were approved to meet ethical standards that ensure information provided will be maintained and handled in a confidential manner. In addition, personal information collected from the population will be protected and treated with similar confidential rigour.

3.4. Population

The population in this study played an important role in the methodology of this research. The researcher used the method of convenience sampling as the target population included specialist civilian and uniformed personnel from SAFIU who have dealt with various cases of money laundering and terrorism financing. Convenience sampling was utilised because there is only one FIU in the KSA, and as such this method was deemed to be useful when a researcher is inclined to describe a specialist group in a particular way (Henry, 1990).

Although there is no clear-cut answer to the correct size for any given research, Cohen et al. (2000) note that 30 is considered the minimum number of cases if researchers plan to use some form of statistical analysis on their data. In this research, the entire population of 111 employees was chosen, as there is only one SAFIU for the whole of Saudi Arabia. Utilising the entire population meant that the results obtained were more reliable. Table 4 provides the summary of the respondents that was utilised in the research. For a complete table of the demographics, refer to Table 7.

Table 4: Demographic Characteristics of Respondents

Description	Respondents
Number of Respondents	74 (66.67% of the entire population)
Type	Officer or Civilian
Age	20-60
Qualification	High school–Master
Courses Attended	0-4
Work Experience	0-20

3.5. Data collection

In this study, semi-structured questionnaires were given to SAFIU staff members. The survey questionnaires were semi-structured, composing predominantly closed ended questions and a few open-ended questions. The questionnaire enabled the researcher to collect quantitative data from a large number of participants simultaneously, thus providing the researcher with an effective tool for data collection (Wellington, 2000). The researcher chose to collect data using questionnaires based on the following reasons:

- The unavailability of publicly available data that analyses the effectiveness of SAFIU
- Obtaining confidential or closed information was difficult due to the nature, content and security clearance required to access information within the organisation.

In addition, the collection of data via questionnaires was the most cost efficient technique, as interviewing each employee within the organisation would adversely affect their day-to-day responsibilities. Further, the researcher wanted to capture the opinions of employees and using other methods based on aggregate data would limit the opportunity to analyse information unique to each individual.

3.6. Designing the questionnaire

The questionnaire consisted of two main sections:

Section A – This section of the questionnaire was dedicated to recording demographic characteristics of the respondents, such as age, qualification, nature of work, experience and proficiency in training courses.

Section B – This section of the questionnaire was allocated a set of questions that enable the respondents to reflect on their views and opinions. These were captured in a summated rating or 'Likert scale'. Developed by Rensis Likert in 1932, the scale ranges from positive to negative and included five categories: 5-strongly agree, 4-agree, 3-neutral, 2-disagree and 1-strongly disagree. Utilising a Likert scale has the advantage of ease in design (Johnson & Christensen 2007). Tittle and Hill (1967) suggest the Likert Scale is the most widely used method of scaling, as it is easy to construct and tends to be more reliable than other scales with the same number of items.

The different sections of the questionnaire were tailored to the objectives and research problems of the study and were broken down into four parts:

Part 1: *What is the effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing?*

Part 2: *What is the effectiveness of SAFIU in administering money laundering combating activities with other government and non-government agencies such as finance and banking institutions?*

Part 3: *What is the effectiveness of the international cooperation of AML and CTF between SAFIU and FIUs in other countries?*

Part 4: *What suggestions can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism finance?*

3.7. Validity and translation of instruments

3.7.1. Validity of instrument

To confirm validity, the questionnaire was provided to four experts to review the constituent items for relevance and clarity. Comments of the reviewers were considered in developing the final edition prior to the translation of instruments. Table 5 provides the details of the experts consulted.

Table 5: Experts Consulted for Validity

Title	Position	Agency	Country
Dr	Professor	SAMA	KSA
Mr	Executive Secretary	MENAFATF	Kingdom of Bahrain
Dr	Professor	Naif Arab University for Security Sciences	KSA
Dr	Legal Expert	Qatar Financial Information Unit	Qatar

3.7.2. Translation of instrument

The study was conducted in the Arabic language in Riyadh city, KSA and the instruments were written in Arabic to overcome any language barriers. Several factors were considered in the process of translation including that the English version and the Arabic translation communicated the same concepts; that the translation was clear and understandable; and finally, to certify the translation. To achieve these requirements, the questionnaires, information to respondents and the consent form were translated into Arabic by a registered National Accreditation Authority for Translators and Interpreters (NAATI) no. 60167 in Melbourne Australia, to ensure subject relevance and consistency.

3.7.3. Pilot study

In order to verify the reliability of the instrument, a pilot study was conducted on 10 SAFIU staff members. Respondents were provided with an Arabic version of the questionnaire rather than an English version based on two reasons: firstly, it was more relevant since the Arabic version was used in the data collection; and secondly, the reliability check on the English version could have been different from the Arabic version because of possible linguistic inconsistencies in the translation.

3.7.4. Reliability of instrument

After receiving the questionnaires from the pilot group, the researcher tested the reliability by using internal consistency method and deriving the alpha coefficient of the questionnaire items after the data had been collected using the Statistical Package for Social Science (SPSS). SPSS is a computer application that provides statistical analysis of data. It allows for in-depth data access and preparation, analytical reporting, graphics and testing using different statistical tests including parametric and non-parametric tests. From 2009, SPSS Inc. changed their product name from SPSS to Predictive Analytics Software (PASW).

One common way of computing correlation values among the questions on the instruments is by using Cronbach's Alpha. Cronbach's Alpha splits all the questions on the instrument in every possible way and computes correlation values for all of them. After several iterations, a number for Cronbach's alpha is generated, and the closer it is to that number, the higher the reliability of the instrument (Cronbach, 1951). While the acceptable value for Cronbach alpha varies among researchers, the researcher followed Perry (2005), who considers a value greater than 0.75 to be appropriate. Table 6 demonstrates the results acquired from testing the reliability of the instrument. Additional suggestions from the pilot study were also collected and incorporated in the instrument.

Table 6: Instrument Reliability Results

Part	Description	No. of questions	Reliability coefficient
1	*The effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing*	29	0.8496
1a	First subsection - the effectiveness of SAFIU in receiving reports	14	0.8473
1b	Second subsection - the Effectiveness of SAFIU in analysing reports	8	0.8204
1c	Third subsection - the effectiveness of SAFIU in administering STRs	7	0.8937
2	*The effectiveness of SAFIU in administering money laundering combating activities with other government and non-government agencies such as finance and banking institutions*	27	0.8849
2a	First subsection - the effectiveness of SAFIU in administering AML activities with government and non-government institutions	18	0.8771
2b	Second subsection - the effectiveness of SAFIU in coordinating AML activities with government and non-government institutions	9	0.898
3	*The effectiveness of the international cooperation of AML and CTF between SAFIU and FIUs in other countries*	10	0.8971
4	*The suggestions that can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism finance*	6	0.9804
All parts and subsections of the research instrument		**72**	**0.9012**

As the table above indicates, the reliability coefficient for all grouped items are greater than 0.75, the value the researcher accepted for the analysis.

3.8. Procedure

In the research process, the data collection follows on from the review of literature. A systematic and precise data collection is pivotal for the subsequent research stage of data analysis and is directly responsible for the accuracy of research findings.

An endorsement letter was provided by SAFIU to enable the study to take place on staff members. A SAFIU staff member was assigned the responsibility of coordinating the room facilities and allocating the appropriate respondents. Due to the operational requirements, the respondents were grouped into three groups, which incorporated the three shifts available: morning, afternoon and evening.

The researcher presented the respondents with the approval and information for respondents sheet, thereby enabling each candidate to be aware of the reason for the study. The researcher provided a verbal brief reiterating the documents provided and purpose of study. In line with the research approval by the ethics committee at Victoria University, all respondents were informed about their consent to collect data. It was stressed that participation in this study was voluntary and that their responses will be held confidentially. The consent form was presented for the respondents to read and consent through formal signing.

At the completion of the survey, the respondents were asked if they had any further questions that they would like clarified. The survey questionnaires were gathered to commence the data analysis phase. Of total respondents, three were not included in the final calculation of data as the questionnaires received from these respondents were incomplete. As such, a total of 74 questionnaires was utilised for the analysis.

3.9. Data analysis

Data analysis is the second-last step in the research process and provides the arguments for the research discussion and the drawing of conclusions. For this study, appropriate non-parametric statistical tests were conducted to analyse the quantitative collected from the questionnaire. Descriptive statistics, such as means, frequencies and standard deviations and Spearman's Rho correlations, were conducted in SPSS. The Spearman's Rho correlation coefficient is a non-parametric approach (Field,

2009), which was preferred as one of the assumptions of parametric approach (interval or ratio level data) was violated.

The Kruskal-Wallis test was also performed to test the differences between groups by age, qualification, work experience and number of training courses attended. The analysis by nature of the work was excluded from the Kruskal-Wallis test, as the job responsibilities for uniformed and civilian personnel overlapped each other. The Kruskal-Wallis test is a non-parametric test used to compare three or more groups of sample data when the assumptions of one-way independent parametric test are violated (Field, 2009). The Kruskal-Wallis test can be applied for ordinal data, as there was no assumption made about the distribution (Jamieson, 2004). The hypothesis for the test is as follows:

- **Null hypothesis:** Null hypothesis assumes that the samples are from identical populations, which means the opinions of different groups by age, qualification, work experience and number of training courses attended do not differ.
- **Alternative hypothesis:** Alternative hypothesis assumes that there is a difference among different population groups by age, qualification, work experience and number of training courses.

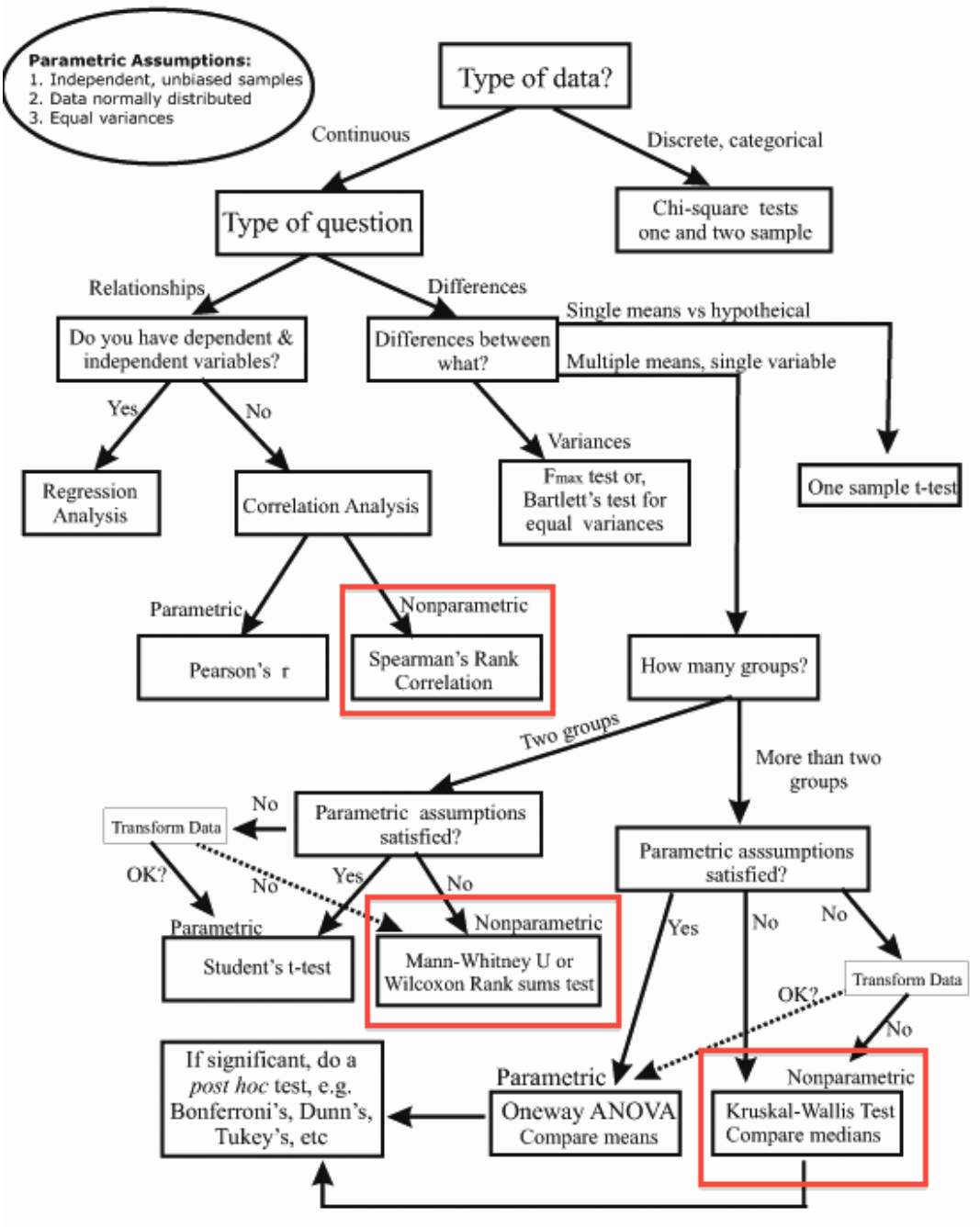
In addition, the Mann-Witney U (Field, 2009) test was utilised to test whether the opinions of civilian and uniformed staff members differed. The Mann-Whitney U test is a non-parametric test used to determine whether two samples of ordinal or ranked data differ. The Mann-Whitney U ranks all the cases for each of the two groups from the lowest to the highest value. Then a mean rank, sum of ranks and 'U' score is computed for each group (Mann & Whitney, 1947). The hypothesis for the test is as follows:

- **Null Hypothesis:** There is no difference in response between civilian and uniformed staff.
- **Alternative Hypothesis:** There is a difference in response between civilian and uniformed staff members.

For qualitative analysis, responses were processed after translation in the Microsoft Excel program, and responses categorised according to the subject matter. Common words from each comment were identified and categorised appropriately to arrive at

the conclusion. The items highlighted with a red box in Figure 6 demonstrates the statistical tests that were conducted to analyse the quantitative results collected (Gerwien, 2008).

Figure 6: Statistical Tests Utilised within the Research Study



Source: Gierwen, 2008

3.10. Limitations of study

This study, like other studies is conducted within a particular framework and as such, it has to be recognised that a number of limitations exist. It should be noted, however,

that the limitations of a study do not necessarily decrease its value or minimise its strength, rather provides boundaries within which the results can be interpreted.

The instruments used in this study are subject to the same criticism made of most self-assessment instruments, that is, such instruments are subjective in nature and may or may not truly reflect the respondent's characteristics. A thorough introduction and explanation of the purpose of the study at the beginning of the data collection attempted to minimise this risk of response error.

It is also important to note that the results of this study are limited to the opinions of male SAFIU staff members located in the city of Riyadh within the calendar year of 2011. Despite these limitations, the results provide a beneficial appreciation on the compliance of SAFIU with the international standards. These limitations also provide the opportunity for consideration during future research and investigative analysis.

3.11. Chapter summary

This chapter detailed the methodology and procedures of this study. After the research design was described, details of the research questions and study were provided. Finally, the procedures were then presented to describe the instruments, validity, translation and process of data collection. The adoption of these methods provided a sound foundation to obtain reliable and valid results. The next chapter (Chapter 4: Findings) reports on the data analysis, and provides results that form the basis of the final discussion chapter.

CHAPTER 4: FINDINGS

4.1. Introduction

This chapter presents a descriptive statistical analysis for the quantitative and qualitative data collected from the respondents. The chapter commences by providing a summary of the demographic characteristics of the study. Quantitative findings are then presented for each research question prior to illustrating the qualitative results acquired. A summary of the chapter is then detailed to provide a platform where the results are analysed and discussed.

4.2. Demographic analysis

The first stage of the data analysis was concerned with the personal and functional characteristics of the study. The questionnaire focused on demographic qualities that had the ability to shape the differences in their perception of the subject matter. Table 7 below demonstrates the study demographic details.

Table 7: Demographic Characteristics of Respondents

No.	Age	Frequency (N)	Percentage
1	Less than 30 years old	28	37.84
2	30 - 39 years old	29	39.19
3	40 - 49 years old	15	20.27
4	50 years old and over	2	2.70

No.	Nature of the work	Frequency (N)	Percentage
1	Uniformed	39	52.70
2	Civilian	35	47.30

No.	Qualification	Frequency (N)	Percentage
1	Secondary or less	6	8.11
2	Diploma	21	28.38
3	Bachelor	44	59.46
4	Master	3	4.05

No.	Years of Work Experience	Frequency (N)	Percentage
1	Less than 5 years	17	22.97
2	5 - 9 years	32	43.24
3	10 - 14 years	10	13.51
4	15 - 19 years	12	16.22
5	20 years and over	3	4.06

No.	No. of Training Courses	Frequency (N)	Percentage
1	None	5	6.76
2	One training course	18	24.32
3	Two training courses	12	16.22
4	Three training courses	21	28.38
5	Four training courses and more	18	24.32

Of 74 respondents, the demographic analysis indicated that 57 staff members (77 per cent) were under the age of 40 years. 39 staff members (53 per cent) consisted of uniformed members, while the remaining 35 members (47 per cent) consisted of civilians. The education level of the study was significantly high, with 65 members (92 per cent) holding a qualification higher than secondary school level. The analysis also demonstrated that 57 staff members (77 per cent) have at least five years of working experience. Finally, the data indicated that 51 members of the respondents (77 per cent) have attended two or more money laundering and terrorism finance training sessions.

4.3. Quantitative and qualitative analysis

This section presents the quantitative and qualitative analysis of the study as responded in the instrument. The results of the Mann-Whitney test for all questions revealed that there is no difference of response to the questionnaires (nature of the work maintained the null hypothesis). Results of this test have been reported in Appendix C along with the descriptive and correlation statistics for each item.

4.3.1. Research question one

The first research question was aimed to identify the effectiveness of SAFIU in receiving, analysing and administering AML and CTF activities. The question was: *what is the effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing?*

In this part, a total number of 29 questions were provided to the respondents. The questions developed were separated into three subsections. The first subsection consisted of 14 questions that measured the effectiveness of SAFIU in receiving STRs related to money laundering and terrorism financing activities. The second subsection consisted of eight questions that measured the effectiveness of SAFIU in analysing

STRs related to money laundering and terrorism financing activities. In the final subsection, seven questions focusing on the effectiveness of SAFIU administration in combating money laundering and terrorism financing activities was presented to the respondents.

4.3.1.1.What is the effectiveness of SAFIU in receiving STRs?

This section presents the respondents perception on the effectiveness of SAFIU in receiving STRs related to money laundering and terrorism financing activities

With an overall average of 4.44, the study demonstrated that SAFIU is perceived to be very effective in receiving STRs related to money laundering and terrorism financing crimes. The three most effective areas were related to items 14 (mean = 4.96), 2 (mean = 4.88), and 13 (mean = 4.85). The respondents also indicated that SAFIU was particularly effective in maintaining authority to obtain required information from SAMA, Saudi Capital Market and other government agencies. In addition, SAFIU was also effective in receiving money laundering and terrorism STRs through various channels. The respondents however, indicated that SAFIU is least effective in receiving and reviewing STRs that are not related to money laundering and terrorism financing activities (mean = 2.99).

4.3.1.2.What is the effectiveness of SAFIU in receiving STRs (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 2 and 7 (test by age group), questions 1, 2, 3 and 6 (test by qualification), questions 1, 2, 3, 6 and (test by number of training course) and questions 1, 2, 3 and 7 (test by years of experience). The results also indicate a difference of opinion for question 12 (test by training at work) where a high variance is contributed by respondents who received four or more training courses at work. Table 8 presents the results of the Kruskal-Wallis test.

Table 8: Kruskal-Wallis Test According to Age, Qualification, Experience and Training Attended

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Age	N	Mean Rank													
< 30 years old	28	32.6	31.4	32.0	41.1	45.0	36.0	42.4	38.3	37.5	39.4	42.1	38.1	41.7	35.0
30 to < 40 years	29	39.4	40.7	37.6	38.2	32.7	35.2	36.1	37.3	34.1	36.0	36.8	35.3	35.3	39.0
40 to < 50 years	15	42.0	42.0	45.1	29.2	31.7	41.6	35.1	37.6	44.6	37.7	33.1	38.7	33.1	39.0
> 50 years	2	44.5	42.0	56.5	38.0	45.8	60.5	8.0	29.0	33.5	31.5	16.5	50.8	43.0	39.0
Chi-Square		5.55	11.32	6.21	3.36	7.19	4.37	11.35	0.59	3.37	0.79	5.26	1.26	5.52	5.07

p-value		0.14	0.01	0.10	0.34	0.07	0.22	0.01	0.90	0.34	0.85	0.15	0.74	0.14	0.17

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Qualification	N	Mean Rank													
Secondary or less	6	19.8	23.5	17.3	43.8	45.7	17.3	45.0	47.5	45.8	50.0	37.8	20.3	43.0	32.8
Diploma	21	37.5	35.0	34.3	39.6	37.8	40.2	38.0	35.2	37.9	34.1	40.2	42.2	37.7	39.0
Bachelor	44	39.5	40.3	41.1	35.6	36.5	38.2	36.6	37.4	36.9	38.2	36.8	37.6	36.3	37.3
Master	3	44.5	42.0	47.7	38.0	33.7	48.7	32.7	35.2	27.3	25.3	28.3	37.5	43.0	39.0
Chi-Square		10.28	11.62	8.97	1.14	1.21	8.62	2.00	2.67	2.26	5.29	1.25	5.41	1.93	3.45
p-value		0.02	0.01	0.03	0.77	0.75	0.03	0.57	0.45	0.52	0.15	0.74	0.14	0.59	0.33

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Training	N	Mean Rank													
None	5	14.9	12.4	18.6	52.0	48.9	20.4	45.0	47.5	44.6	50.0	44.9	23.8	43.0	31.6
1 course	18	34.2	33.8	27.9	33.9	40.1	31.6	40.9	37.2	37.6	35.6	36.6	30.1	40.9	36.9
2 courses	12	32.2	38.9	29.3	34.8	34.2	42.8	38.8	41.3	33.5	43.8	39.0	29.8	36.8	39.0
3 courses	21	42.7	42.0	45.0	40.1	40.2	37.4	38.0	36.9	37.9	39.4	38.5	42.7	36.0	39.0
4 and more	18	44.5	42.0	49.1	35.9	30.8	44.7	30.6	33.1	37.6	29.4	34.3	47.8	34.8	36.9
Chi-Square		21.36	28.42	20.00	3.74	4.61	9.68	6.10	3.77	1.35	8.29	1.55	12.43	3.15	4.81
p-value		0.00	0.00	0.00	0.44	0.33	0.05	0.19	0.44	0.85	0.08	0.82	0.01	0.53	0.31

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Experience	N	Mean Rank													
< 5 years	17	27.1	26.8	26.2	39.9	43.6	30.6	40.6	38.8	38.9	41.3	40.7	30.5	43.0	34.6
5 to < 10 years	32	38.7	39.7	37.3	40.0	38.2	38.7	40.4	38.3	34.7	39.6	38.9	37.1	37.2	37.8
10 <15 years	10	44.5	42.0	45.9	35.5	26.2	35.7	33.9	36.4	37.2	27.8	41.4	48.9	35.6	39.0
15 to < 20 years	12	41.4	42.0	44.5	29.0	39.7	45.7	26.5	35.2	42.8	37.7	28.3	39.0	36.8	39.0
20 years and over	3	44.5	42.0	47.7	38.0	23.8	36.8	45.0	35.2	39.7	25.3	28.3	37.5	18.3	39.0
Chi-Square		12.74	17.66	9.63	2.84	6.39	4.87	9.73	0.51	1.93	5.70	4.86	5.22	9.45	3.68
p-value		0.013	0.001	0.047	0.585	0.172	0.301	0.045	0.972	0.748	0.222	0.302	0.266	0.051	0.452

4.3.1.3.What is the effectiveness of SAFIU in analysing STRs ?

This section presents the respondents perception on the effectiveness of SAFIU in analysing STRs on money laundering and terrorism financing activities.

Results analysed from the respondents indicated that SAFIU is perceived to be very effective in analysing STRs overall average of 4.57. The three most effective areas were related to items 1 (mean = 4.97), 6 (mean = 4.92) and 7 (4.89). The average of 4.57 indicates that SAFIU effectively classifies STRs according to the suspicious nature of money laundering and terrorism financing activities. In addition, the respondents highlighted that SAFIU was effective in coordinating the analysis of information from financial and security specialists. Furthermore, the results deemed that SAFIU is also effective in maintaining authority to obtain information from banks, regardless of the privacy laws that exist. On the other hand, SAFIU was perceived to be least effective in providing sufficient staff to analyse the volume of reports received (mean = 3.73).

4.3.1.4.What is the effectiveness of SAFIU in analysing STRs (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 percent (0.05) significance level for question 7 (test by qualification) and questions 1, 7 and 8 (test

by number of training courses). This result is ignored as a majority of respondents strongly agreed with the statement. As such, the Kruskal-Wallis test indicates that there is no group differences in the effectiveness of analysing STRs as indicated in Table 9.

Table 9: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Age	N	Mean Rank							
Less than 30 years old	28	38.5	32.8	36.4	38.0	37.6	36.5	34.9	35.7
From 30 to less than 40 years old	29	35.9	40.7	38.3	35.6	37.0	36.7	37.7	36.1
From 40 to less than 50 years old	15	38.5	39.5	39.1	37.3	36.2	40.5	41.5	44.1
From 50 years old and over	2	38.5	42.0	29.5	58.5	53.0	40.5	41.5	33.5
Chi-Square		3.15	6.99	0.59	2.70	1.49	1.92	3.46	1.98
p-value.		0.37	0.07	0.90	0.44	0.68	0.59	0.33	0.58

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Qualification	N	Mean Rank							
Secondary or less	6	38.5	29.7	32.2	29.8	35.0	28.2	16.8	17.7
Diploma	21	38.5	40.2	42.1	39.4	37.6	40.5	41.5	38.7
Bachelor	44	36.8	37.0	36.6	37.8	36.8	37.1	38.1	38.7
Master	3	38.5	42.0	29.5	35.5	53.0	40.5	41.5	50.5
Chi-Square		1.38	4.04	2.21	1.24	2.28	7.20	22.15	7.12
p-value		0.71	0.26	0.53	0.74	0.52	0.07	0.00	0.07

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Training	N	Mean Rank							
None	5	38.5	34.6	31.1	30.9	24.2	40.5	26.7	19.8
One training course	18	38.5	31.7	36.2	32.4	35.0	34.3	33.3	28.3
Two training courses	12	32.3	38.9	28.8	29.1	35.4	34.3	35.3	28.8
Three training courses	21	38.5	38.5	36.7	44.4	41.0	40.5	41.5	47.1
Four training courses and more	18	38.5	42.0	47.3	42.0	41.0	38.4	41.5	46.3
Chi-Square		10.48	7.09	7.58	7.83	4.44	5.33	11.84	17.54
p-value		0.03	0.13	0.11	0.10	0.35	0.26	0.02	0.00

*Grouping Variable:		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Experience	N	Mean Rank							
Less than 5 years	17	38.5	33.3	29.5	32.9	31.8	36.1	30.6	27.5
From 5 to less than 10 years	32	36.2	37.4	38.5	35.6	38.5	35.9	38.0	37.8
From 10 to less than 15 years	10	38.5	42.0	51.9	51.6	42.2	40.5	41.5	46.3
From 15 to less than 20 years	12	38.5	38.9	33.5	34.9	38.0	40.5	41.5	40.3

From 20 years and over	3	38.5	42.0	40.2	47.0	41.0	40.5	41.5	50.5
Chi-Square		2.66	3.97	9.00	7.66	2.45	3.29	9.07	7.38
p-value		0.616	0.410	0.061	0.105	0.654	0.510	0.059	0.117

4.3.1.5.What is the effectiveness of SAFIU in managing STR activities ?

This section presents the respondents perception on the effectiveness of SAFIU in managing activities related to money laundering and terrorism finance.

The respondents indicated that SAFIU is very effective in managing administrative duties related to money laundering and terrorism finance. The three most effective areas were related to items 1 (mean = 4.97), 2 (mean = 4.92) and 7 (mean = 4.59). The average indicated that SAFIU is particularly effective in securing information, coordinating SAFIU divisions and in using relevant research and case studies to develop unit action plans. SAFIU however was perceived to be least effective in providing additional training for staff members (mean = 4.04).

Overall, the respondents indicated that there is a high effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing with a mean of 4.51. The degree of effectiveness is classified as follows:

- The effectiveness of SAFIU in receiving STRs rated an average of 4.44.
- The effectiveness of SAFIU in analysing STRs rated an average of 4.57.
- The effectiveness of SAFIU in managing activities rated an average of 4.51.

In addition to the quantitative data, the study also provides a number of comments regarding the effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing. 10 respondents (7.4 per cent) commented that SAFIU is not analysing STRs that are not related to money laundering and terrorism finance. They claimed that SAFIU considers such transactions as not part of its area of interest and allocates them a low priority.

Seven respondents (5.18 per cent) commented that the number of staff allocated to receiving STRs is insufficient when compared to the volume of reports received. Additionally, four respondents (2.96 per cent) stated that some employees require retraining. Three respondents (2.22 per cent) also reported that SAFIU should

introduce electronic systems for receiving STRs to enable secure and quicker submission whilst eliminating the possibility of errors with paper based reports. Finally, three respondents (2.22 per cent) commented that occasionally, SAFIU receives STRs that are not related to money laundering and terrorism finance.

4.3.1.6.What is the effectiveness of SAFIU in managing STRs (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 6 and 7 (test by qualification) and questions 5 and 6 (test by number of training). The results indicate that the extent of training required depends on the employees' educational background. The results also demonstrate that staff members who received more training become more acquainted with the sources of money laundering and the terrorism finance. There was no difference by age groups and years of experience as shown in Table 10.

Table 10: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7
Age	N	Mean Rank						
Less than 30 years old	28	38.5	35.2	34.8	38.1	37.4	38.1	38.0
From 30 to less than 40 years old	29	35.9	37.9	40.5	37.5	33.6	31.2	35.9
From 40 to less than 50 years old	15	38.5	40.5	38.2	36.3	44.6	47.8	40.2
From 50 years old and over	2	38.5	40.5	26.5	38.8	42.8	43.8	34.0
Chi-Square		3.15	2.95	1.93	0.09	3.24	7.06	0.63
p-value		0.37	0.40	0.59	0.99	0.36	0.07	0.89

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7
Qualification	N	Mean Rank						
Secondary or less	6	38.5	28.2	28.3	44.7	22.9	20.3	15.5
Diploma	21	38.5	40.5	35.9	33.6	37.9	44.8	40.2
Bachelor	44	36.8	37.1	40.3	39.5	38.6	35.6	39.0
Master	3	38.5	40.5	26.5	21.0	48.2	48.7	40.2
Chi-Square		1.38	7.20	3.31	4.49	4.37	8.58	9.51
p-value		0.71	0.07	0.35	0.21	0.22	0.04	0.02

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7
Training	N	Mean Rank						
None	5	38.5	33.1	22.1	49.4	22.2	23.6	22.9
One training course	18	36.4	32.3	35.1	35.7	32.6	32.2	40.2
Two training courses	12	35.4	37.4	38.4	38.8	32.0	32.7	34.0

Three training courses	21	38.5	40.5	40.6	34.4	37.9	40.0	36.6
Four training courses and more	18	38.5	40.5	39.9	38.8	50.0	47.0	42.2
Chi-Square		3.18	9.08	4.28	2.81	12.49	8.76	5.25
p-value		0.53	0.06	0.37	0.59	0.01	0.07	0.26

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7
Experience	N	Mean Rank						
Less than 5 years	17	38.5	34.0	30.4	38.7	31.6	33.1	32.9
From 5 to less than 10 years	32	36.2	37.0	41.6	39.3	36.7	34.9	39.8
From 10 to less than 15 years	10	38.5	40.5	41.9	35.2	42.8	40.8	37.7
From 15 to less than 20 years	12	38.5	40.5	32.9	34.2	43.7	42.6	40.2
From 20 years and over	3	38.5	40.5	37.5	32.8	37.3	58.5	27.8
Chi-Square		2.66	4.29	4.90	1.03	3.50	5.69	2.66
p-value		0.616	0.368	0.298	0.905	0.477	0.224	0.616

4.3.2. Research question two

The second research question was aimed to identify the effectiveness of SAFIU in coordinating activities with other agencies. The question was: *What is the effectiveness of SAFIU in administering money laundering combating activities with other government and non-government agencies such as finance and banking institutions?.*

Part two of the questionnaire consisted of 27 questions. The first subsection consisted of 18 questions tailored to measure the effectiveness of SAFIU in administering activities that combat money laundering and terrorism finance activities with other governmental and non-governmental agencies. The second subsection consisted of nine questions aimed to measure the effectiveness of SAFIU in coordinating activities that combat money laundering and terrorism finance crimes with other government and non-governmental agencies.

4.3.2.1.What is the effectiveness of SAFIU in administering activities with government and non-government institutions?

This section presents the respondents perception on the effectiveness of SAFIU in administering money laundering and terrorism financing crimes with other government and non-government agencies such as finance and banking institutions.

Analysis from the respondents indicated that SAFIU is very effective in controlling money laundering and terrorism financing crimes with other governmental and non-governmental agencies, such as banks and other financial institutions, with an overall average of 4.48. The three most effective areas were related to items 3 (mean = 5), 13 (mean = 5) and 12 (mean = 4.97). Results indicated that SAFIU is particularly effective in accessing law enforcement information, as well as confiscating property and freezing accounts that are associated with money laundering or terrorism financing activities. In addition, SAFIU is also considered effective in ensuring that the roles and responsibilities of government agencies are clear and specific. In relation to disseminating the latest information on money laundering and terrorism financing activities to government and non-government agencies, SAFIU was deemed least effective (mean = 3.85).

4.3.2.2.What is the effectiveness of SAFIU in administering activities with government and non-government institutions (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 2, 11, 16, 17 and 18 (test by number of training). The null hypothesis could not be rejected for other groupings, which suggests that staff members become more knowledgeable when provided with training. Table 11 demonstrates the effectives of SAFIU in administering activities with government and non-government institutions.

Table11: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Age	N	Mean Rank																	
< 30 years	28	36.3	38.2	37.5	37.4	35.7	37.6	34.6	36.4	39.0	41.0	37.0	35.9	37.5	36.9	36.1	38.1	35.5	37.6
30 < 40 years	29	34.1	37.8	37.5	32.5	37.2	33.0	37.4	37.7	34.3	34.2	35.6	38.5	37.5	37.1	36.4	34.4	34.4	33.2
40 < 50 years	15	45.8	34.9	37.5	44.4	41.0	47.6	42.5	39.0	40.4	36.9	40.9	38.5	37.5	38.6	41.1	43.3	45.2	44.0
50 and >	2	40.0	43.5	37.5	59.0	41.0	26.0	42.5	39.0	40.5	40.5	46.0	38.5	37.5	43.5	46.5	30.5	51.5	49.5
Chi-Square		4.62	0.62	0.00	6.19	2.53	7.30	4.10	1.41	1.90	1.96	1.73	3.33	0.00	0.55	1.72	2.19	4.80	4.66
p-value		0.20	0.89	1.00	0.10	0.47	0.06	0.25	0.70	0.59	0.58	0.63	0.34	1.00	0.91	0.63	0.53	0.19	0.20

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Qualification	N	Mean Rank																	
Secondary or less	6	34.6	37.3	37.5	22.4	28.7	32.0	36.3	32.8	40.3	43.0	28.2	32.3	37.5	31.2	29.4	25.3	29.0	29.0
Diploma	21	39.8	32.0	37.5	43.3	39.2	38.0	39.0	39.0	44.9	37.9	42.7	38.5	37.5	41.7	43.3	40.8	43.6	46.2
Bachelor	44	35.3	40.1	37.5	35.3	37.6	38.8	36.6	37.3	33.4	35.1	35.7	37.7	37.5	35.9	35.2	37.4	34.8	33.7
Master	3	60.0	37.3	37.5	59.0	41.0	26.0	42.5	39.0	40.5	58.5	46.0	38.5	37.5	43.5	46.5	40.3	51.5	49.5
Chi-Square		6.16	3.00	0.00	9.66	4.79	2.02	1.01	3.45	7.61	5.00	5.80	5.08	0.00	4.42	6.02	2.84	6.15	9.78
p-value		0.10	0.39	1.00	0.02	0.19	0.57	0.80	0.33	0.05	0.17	0.12	0.17	1.00	0.22	0.11	0.42	0.10	0.02

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Training	N	Mean Rank																	
None	5	33.5	25.0	37.5	21.7	33.6	26.0	35.1	39.0	32.6	51.3	39.8	38.5	37.5	36.1	37.8	31.3	42.1	41.3
1 course	18	34.6	39.4	37.5	41.3	32.8	38.0	34.3	34.9	38.6	37.3	29.9	34.4	37.5	33.2	32.1	31.4	29.8	28.7
2 courses	12	34.4	34.3	37.5	30.8	34.8	27.9	39.4	39.0	23.6	28.5	29.2	38.5	37.5	34.3	33.5	25.3	30.5	27.6
3 courses	21	41.0	46.1	37.5	37.5	41.0	41.4	37.2	37.2	41.6	40.4	40.9	38.5	37.5	38.2	39.5	40.3	36.4	40.9
4 courses >	18	39.6	31.2	37.5	42.5	41.0	42.0	40.4	39.0	42.2	36.5	46.0	38.5	37.5	43.5	43.2	50.2	49.9	47.9
Chi-Square		2.21	10.51	0.00	6.59	8.75	7.53	2.57	3.76	12.34	6.00	13.72	6.31	0.00	5.96	5.32	14.09	12.99	15.33
p-value		0.70	0.03	1.00	0.16	0.07	0.11	0.63	0.44	0.01	0.20	0.01	0.18	1.00	0.20	0.26	0.01	0.01	0.00

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Experience	N	Mean Rank																	
< 5 years	17	36.2	35.9	37.5	35.1	32.3	36.6	36.0	34.6	36.2	42.4	33.8	34.1	37.5	34.8	35.4	34.1	33.2	34.0
5 < 10	32	33.6	40.0	37.5	36.0	37.5	35.7	35.6	39.0	34.0	36.5	35.2	38.5	37.5	36.6	35.1	33.3	34.6	34.3
10 < 15	10	39.8	32.4	37.5	35.9	41.0	36.8	38.8	35.3	46.7	29.7	46.0	38.5	37.5	43.5	43.6	54.1	42.7	43.7
15 < 20	12	44.8	40.4	37.5	40.7	41.0	41.0	42.5	39.0	40.4	37.5	39.7	38.5	37.5	37.3	39.8	39.1	43.7	42.7
20 and >	3	50.0	25.0	37.5	59.0	41.0	50.0	42.5	39.0	40.5	46.5	46.0	38.5	37.5	43.5	46.5	40.3	51.5	49.5
Chi-Square		5.45	3.48	0.00	4.48	6.45	2.26	3.40	5.42	5.39	3.69	5.58	6.80	0.00	3.29	3.59	8.89	5.47	5.28
p-value		0.244	0.481	1.000	0.344	0.168	0.689	0.493	0.247	0.250	0.449	0.233	0.147	1.000	0.510	0.465	0.064	0.243	0.260

4.3.2.3.What is the effectiveness of SAFIU in coordinating activities with government and non-government institutions ?

This section presents the respondents perceptions of the effectiveness of SAFIU in coordinating activities related to combat of money laundering and terrorism finance crimes with governmental and non-governmental agencies such as banks and other financial institutions.

The data collected indicates that respondents perceive SAFIU to be very effective in coordinating activities related to the combating of money laundering and terrorism

finance crimes with governmental and non-governmental agencies, such as banks and other financial institutions, with an overall average of 4.41. The three most effective areas were related to items 3 (mean = 4.97), 9 (mean = 4.77) and 4 (mean = 4.69). The results suggest that SAFIU is particularly effective in exchanging information regarding money laundering and terrorism finance with other domestic government agencies, as well as cooperating with authorities in investigations of money laundering and terrorism financing activities. Furthermore, the analysis demonstrated that SAFIU is effective in freezing accounts on requests from AML units of SAMA, MOCI and MOJ associated with money laundering and terrorism financing activities. On the other hand, SAFIU was least effective in providing training programs to financial and non-financial institutions (mean = 4.12).

In summarising the quantitative results, SAFIU is perceived by respondents as being very effective in administering money laundering and terrorism financing crimes with other government and non-government agencies, such as finance and banking institutions, with an overall average of 4.45. The degree of effectiveness is classified as follows:

- The effectiveness of SAFIU in controlling money laundering and terrorism financing crimes with other governmental and non-governmental agencies such as banks and other financial institutions with an average of 4.48.
- The effectiveness of SAFIU in coordinating activities related to combat of money laundering and terrorism finance crimes with governmental and non-governmental agencies such as banks and other financial institutions with average of 4.41.

The respondents also provided a number of comments for this section. 9 respondents (6.66 per cent) indicated that some staff members of banks and commercial companies' lack knowledge of the reporting indicators and requirements to combat money laundering and terrorism financing, while 6 respondents (4.44 per cent) commented that the PCCML is not providing sufficient support to SAFIU. In terms of performance, 3 respondents (2.22 per cent) commented that SAFIU does not issue periodic reports that include samples of case studies, performance and statistics of cases.

Lastly, one member (0.74 per cent) reported that the training SAFIU conducts for staff members in banks and non-financial institutions is irregular and not consistent.

4.3.2.4.What is the effectiveness of SAFIU in coordinating activities with government and non-government institutions (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 3, 4 and 8 (test by qualification) and question 4, 5 and 6 (test by training). Results indicated that respondents with lower qualifications and less number of training courses attended skewed towards neutral or disagreeing with the statement and, this may be due to the responsibility or authority assigned to each employee. Table 12 demonstrates the effectives of SAFIU in coordinating activities with government and non-government institutions.

Table 12: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Age	N	Mean Rank								
Less than 30 years old	28	40.2	34.7	35.9	38.1	38.0	31.9	32.7	34.6	37.8
From 30 to less than 40 years old	29	34.5	34.3	38.5	34.6	34.9	37.8	39.0	37.6	36.4
From 40 to less than 50 years old	15	35.3	46.2	38.5	40.9	40.6	46.8	41.0	41.8	38.5
From 50 years old and over	2	60.0	58.5	38.5	46.0	45.0	41.3	57.5	44.5	43.0
Chi-Square		4.68	7.43	3.33	2.31	2.01	5.91	4.63	1.56	0.64
p-value.		0.20	0.06	0.34	0.51	0.57	0.12	0.20	0.67	0.89

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Qualification	N	Mean Rank								
Secondary or less	6	35.3	27.7	26.2	27.6	32.3	26.7	19.7	22.5	30.8
Diploma	21	33.6	33.8	38.5	44.0	43.5	38.9	41.8	47.0	41.4
Bachelor	44	39.8	40.0	38.5	35.2	34.8	37.7	37.3	34.2	36.2
Master	3	35.3	46.2	38.5	46.0	45.0	46.8	46.0	49.7	43.0
Chi-Square		1.82	4.00	22.98	7.71	6.18	2.67	6.80	10.64	4.27
p-value		0.61	0.26	0.00	0.05	0.10	0.44	0.08	0.01	0.23

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Training	N	Mean Rank								
None	5	23.0	21.5	38.5	39.2	36.9	20.4	29.9	30.3	36.2
One training	18	39.4	33.8	34.4	31.4	32.9	34.1	34.2	32.8	36.7
Two training	12	44.6	40.0	38.5	28.3	28.7	26.7	35.7	32.7	30.3
Three training	21	35.3	39.1	38.5	40.3	40.1	44.3	39.2	38.5	37.9

Four training and more	18	37.4	42.1	38.5	46.0	45.0	45.0	42.2	46.2	43.0
Chi-Square		5.50	5.95	6.31	12.75	10.81	13.40	2.64	5.89	6.73
p-value		0.24	0.20	0.18	0.01	0.03	0.01	0.62	0.21	0.15

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Experience	N	Mean Rank								
Less than 5 years	17	38.2	30.2	34.1	35.0	36.1	26.8	34.0	29.1	36.7
From 5 to less than 10 years	32	36.9	37.7	38.5	34.6	34.5	37.6	34.7	36.8	35.8
From 10 to less than 15 years	10	41.5	36.3	38.5	46.0	45.0	41.3	43.7	47.6	43.0
From 15 to less than 20 years	12	38.4	49.3	38.5	39.6	39.5	44.0	42.7	37.3	37.3
From 20 years and over	3	23.0	33.8	38.5	46.0	45.0	58.0	46.0	60.0	43.0
Chi-Square		2.49	7.68	6.80	5.50	4.85	10.27	3.75	9.54	2.84
p-value		0.647	0.104	0.147	0.239	0.304	0.036	0.441	0.049	0.586

4.3.3. Research question three

The third research question was aimed to identify the effectiveness of SAFIU in cooperating with foreign FIUs. The question was: *What is the effectiveness of the international cooperation of AML and CTF between SAFIU and FIUs in other countries?*

In part three of the questionnaire, staff members responded to 10 questions that measured the effectiveness of SAFIU in cooperating with other global FIUs.

4.3.3.1.What is the effectiveness of SAFIU in cooperating internationally with other FIUs?

This section presents the respondents perceptions of the effectiveness of the international cooperation of AML and CFT actions between SAFIU and FIUs in other countries.

Results from the study evidenced that SAFIU has a high level of effectiveness when cooperating internationally between SAFIU and other foreign FIUs with an overall average of 4.20. The three most effective areas were related to items 2 (mean = 4.93), 10 (mean = 4.88) and 6 (mean = 4.57). The analysis indicated that SAFIU is most effective in exchanging information with FIUs in other countries through the Egmont Group, as well as being clear on regulations of tracking money laundering and terrorism financing transactions. Additionally, SAFIU is deemed effective in maintaining a database of individuals suspected of money laundering and terrorism

financing activities, at an international level. The results however also implied that SAFIU does not regularly meet with personnel from other FIUs (mean = 3.39).

Qualitative data on the effectiveness of the international cooperation of AML and CTF between SAFIU and FIUs in other countries was also analysed. 12 respondents (8.88 per cent) commented that SAFIU employees need to regularly visit FIUs in other countries, thereby enabling them to be familiar with policies that combat these crimes. 11 respondents (8.14 per cent) highlighted that meetings between SAFIU representatives and officials in other foreign FIUs is irregular, while 10 respondents (7.4 per cent) annotated on the lack of continuous programmes that transfer staff members between SAFIU and other international FIUs. Finally, three respondents (2.22 per cent) commented that SAFIUs exchange of information with FIUs of non-Egmont Group exists but is ineffective and not to the required level.

4.3.3.2.What is the effectiveness of SAFIU in cooperating internationally with other FIUs (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 1 for all grouping variables. The major contributor to the variance was the highest age group, the highest qualification level, and the group that received four or more training courses. This test confirmed that exchange of information is performed as per the allocated responsibility and authority. Table 13 demonstrates the results acquired.

Table 8: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Age	N	Mean Rank									
Less than 30 years old	28	30.6	37.4	34.6	36.9	34.5	39.0	40.6	39.5	41.3	36.7
From 30 to less than 40 years old	29	36.4	36.2	37.4	37.6	37.9	38.2	33.3	34.4	32.6	38.2
From 40 to less than 50 years old	15	50.1	40.0	42.7	38.3	39.7	31.3	40.4	40.4	40.4	37.1
From 50 years old and over	2	55.5	40.0	40.5	39.5	57.0	53.5	33.0	32.8	33.3	42.0
Chi-Square		11.21	1.81	1.87	0.08	3.14	3.41	2.50	1.52	3.27	0.50
p-value		0.01	0.61	0.60	0.99	0.37	0.33	0.48	0.68	0.35	0.92

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Qualification	N	Mean Rank									
Secondary or less	6	10.8	40.0	28.5	39.5	26.2	28.8	38.1	36.9	35.8	29.7
Diploma	21	42.7	40.0	36.9	36.9	39.4	37.6	43.6	46.0	44.8	40.2

Bachelor	44	37.4	35.8	38.4	37.8	37.7	39.2	34.5	33.5	34.3	37.0
Master	3	55.5	40.0	46.5	33.3	44.7	28.8	37.2	37.0	37.3	42.0
Chi-Square		14.90	3.61	2.19	0.26	2.89	2.36	3.04	5.94	4.18	4.04
p-value		0.00	0.31	0.53	0.97	0.41	0.50	0.39	0.11	0.24	0.26

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Training	N	Mean Rank									
None	5	13.4	40.0	36.9	50.6	27.4	31.3	52.6	52.9	52.5	34.6
One training course	18	29.2	37.9	31.3	31.3	36.4	39.1	30.4	32.8	31.9	33.8
Two training courses	12	30.6	33.8	31.5	33.3	44.7	38.1	29.6	30.3	29.5	38.9
Three training courses	21	40.2	36.5	36.9	40.4	37.6	41.2	40.0	37.6	38.8	36.7
Four training courses and more	18	53.9	40.0	48.5	39.5	36.4	32.9	42.7	42.7	42.8	42.0
Chi-Square		24.93	3.78	9.38	5.86	3.37	2.64	8.89	7.24	7.82	4.67
p-value		0.00	0.44	0.05	0.21	0.50	0.62	0.06	0.12	0.10	0.32

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Experience	N	Mean Rank									
Less than 5 years	17	25.7	40.0	33.1	36.2	33.1	33.9	39.8	40.9	40.4	37.6
From 5 to less than 10 years	32	33.1	34.2	34.2	38.3	37.3	40.8	34.0	33.4	33.6	36.2
From 10 to less than 15 years	10	52.7	40.0	51.3	39.5	38.5	38.7	43.0	43.0	43.1	42.0
From 15 to less than 20 years	12	48.7	40.0	38.8	39.5	44.7	35.0	37.1	37.0	37.0	35.8
From 20 years and over	3	55.5	40.0	46.5	21.0	32.3	28.8	45.5	45.5	45.5	42.0
Chi-Square		19.87	6.94	8.07	2.78	3.01	2.58	2.55	3.26	2.92	2.36
p-value		0.001	0.139	0.089	0.595	0.556	0.631	0.636	0.515	0.572	0.670

4.3.4. Research question four

The fourth research question was aimed to discover possible solutions that could improve policies. These suggestions were obtained during the literature review and were presented as a mechanism to deduce whether the proposed suggestions would have any impact on SAFIUs effectiveness and compliance. The question was: *What are the suggestions that can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism financing activities?.*

In part four of the questionnaire, the respondents responded to six questions that measured their opinion of approaches that could be utilised to ensure that policies better detect money laundering and terrorism finance crimes.

4.3.4.1.What are the suggestions that can be provided for SAFIU to develop better policies?

This section presents the respondents suggestions to SAFIU that can perhaps enable the organisation to develop policies that better detect and combat money laundering and terrorism finance.

The results highlighted that there is a need for SAFIU to incorporate suggestions that enable them to develop policies that better detect and combat money laundering and terrorism finance, rated an average of 4.73. The three most rated areas were related to items 1 (mean = 5), 3 (mean = 4.95) and 2 (mean = 4.81). The data indicated that SAFIU staff members feel that the MOI effectively provides financial, technical and resources necessary to enhance the performance of SAFIU. Respondents also agreed with the suggestion that signing MOUs with foreign FIUs to increase cooperation and collaboration will increase efficiency. Furthermore, it was reflected that SAFIU should be permitted to directly access information pertaining to financial institutions.

4.3.4.2.What suggestions can be offered for SAFIU to develop better policies (Kruskal-Wallis Test)?

In the Kruskal-Wallis test, the null hypothesis was rejected at 5 per cent (0.05) significance level for question 4 and 6 (test by age, experience), question 4 (test by qualification) and question 6 (test by training attended). As most of the respondents agreed with the statements, it was concluded that there is no difference of opinion between the different groups. Table 14 demonstrates the results acquired from the respondents.

Table 14: Kruskal-Wallis Test According to Age, Qualification, Training Attended and Experience

Grouping Variable	N	Q1	Q2	Q3	Q4	Q5	Q6
Age	Mean Rank						
Less than 30 years old	28	37.5	37.9	36.9	29.6	33.4	27.4
From 30 to less than 40 years old	29	37.5	39.4	38.2	36.9	39.2	41.0
From 40 to less than 50 years old	15	37.5	34.6	37.0	51.1	42.2	47.6
From 50 years old and over	2	37.5	26.0	39.5	56.0	36.0	52.5
Chi-Square			2.33	0.54	15.04	2.60	15.51
p-value			0.51	0.91	0.00	0.46	0.00

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6
Qualification	N	Mean Rank					
Secondary or less	6	37.5	38.3	39.5	19.0	29.8	21.7
Diploma	21	37.5	42.7	39.5	41.9	36.9	36.6
Bachelor	44	37.5	36.1	36.1	36.7	38.5	39.0
Master	3	37.5	19.8	39.5	56.0	42.2	52.5
Chi-Square			7.54	2.84	10.14	1.37	6.87
p-value			0.06	0.42	0.02	0.71	0.08

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6
Training	N	Mean Rank					
None	5	28.5	27.9	24.9	17.5	26.7	14.5
One training course	18	28.5	28.8	28.9	25.3	27.9	25.4
Two training courses	12	28.5	26.5	30.5	31.5	27.2	28.5
Three training courses	21	28.5	29.5	27.8	32.2	30.2	34.5
Chi-Square			0.62	2.37	6.21	0.51	9.57
p-value			0.89	0.50	0.10	0.92	0.02

Grouping Variable		Q1	Q2	Q3	Q4	Q5	Q6
Experience	N	Mean Rank					
Less than 5 years	17	37.5	38.0	37.3	27.7	28.4	24.2
From 5 to less than 10 years	32	37.5	37.6	37.2	32.9	39.5	36.3
From 10 to less than 15 years	10	37.5	44.5	39.5	48.6	43.4	48.8
From 15 to less than 20 years	12	37.5	29.1	36.4	49.8	42.2	46.3
From 20 years and over	3	37.5	44.5	39.5	56.0	29.8	52.5
Chi-Square		0.00	7.00	0.98	18.45	6.74	17.75
p-value		1.000	0.136	0.912	0.001	0.150	0.001

4.4. Further analysis of the Kruskal-Wallis test

In order to support the overall conclusions of the findings, the Kruskal-Wallis test was performed and identified that some questions were affected by respondents' age, qualification, number of trainings and years of experience for questions. Table 15 represents the questions which established significant differences according to the Kruskal-Wallis test[1].

Table 15: Distribution of Mean by Age, Qualification, Number of Training and Experience Grouping

Q	**Questions**	**GROUP**	**MEAN**
1	SAFIU should operate their offices in major cities.	Less than 30 years old	4.29
		From 30 to less than 40 years old	4.48
		From 40 to less than 50 years old	4.87
		50 years old and over	5.00
2	SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Less than 30 years old	4.32
		From 30 to less than 40 years old	4.69
		From 40 to less than 50 years old	4.87
		50 years old and over	5.00
3	SAFIU receives and reviews STRs that are	Secondary or less	3.17

[1] Only reported questions with significant importance for further disaggregation are included in this table. The complete finding is attached in Appendix D.

Q	Questions	GROUP	MEAN
	not related to money laundering and terrorism finance.	Diploma	3.05
		Bachelor	2.93
		Master	4.00
4	SAFIU provides additional training to all staff members.	Secondary or less	3.33
		Diploma	4.48
		Bachelor	3.89
		Master	4.67
5	Businesses have advanced awareness and knowledge of the danger of money laundering and the terrorism financing.	Secondary or less	3.00
		Diploma	4.76
		Bachelor	3.75
		Master	5.00
6	SAFIU provides training programs to financial and non-financial institutions to understand money laundering and terrorism financing rules and regulations.	Secondary or less	3.67
		Diploma	4.52
		Bachelor	3.95
		Master	4.67
7	SAFIU has to provide guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Secondary or less	4.17
		Diploma	4.57
		Bachelor	4.64
		Master	5.00
8	SAFIU provides training programs to financial and nonfinancial institutions to understand money laundering and terrorism financing rules and regulations.	Less than 5 years	3.76
		From 5 to less than 10 years	4.06
		From 10 to less than 15 years	4.60
		From 15 to less than 20 years	4.17
9	SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Less than 5 years	4.24
		From 5 to less than 10 years	4.56
		From 10 to less than 15 years	4.90
		From 15 to less than 20 years	4.83
10	SAFIU receives and reviews STRs that are not related to money laundering and terrorism finance.	None	3.60
		One training course	2.78
		Two training courses	2.92
		Three training courses	3.10
		Four training courses and more	2.94
11	SAFIU recruits qualified and experienced personnel who possess the required skills in financial analysis.	None	4.00
		One training course	4.17
		Two training courses	3.92
		Three training courses	4.19
		Four training courses and more	4.56
12	SAFIU staff members are informed about the sources of money laundering and the terrorism finance.	None	3.80
		One training course	4.11
		Two training courses	4.08
		Three training courses	4.33
		Four training courses and more	4.72
13	SAFIU disseminates latest information regarding money laundering and terrorism finance received to fellow government agencies.	None	3.40
		One training course	3.94
		Two training courses	3.33
		Three training courses	4.00
		Four training courses and more	4.06

Q	Questions	GROUP	MEAN
14	SAFIU regularly releases periodic reports which include statistics, typologies and trends as well as information regarding its activities.	None	4.80
		One training course	4.22
		Two training courses	4.00
		Three training courses	4.76
		Four training courses and more	5.00
15	The Saudi Permanent Committee on Combating Money Laundering (PCCML) supports SAFIU's objectives.	None	3.60
		One training course	3.50
		Two training courses	3.00
		Three training courses	4.14
		Four training courses and more	4.67
16	Financial institutions have awareness and knowledge of the danger of money laundering and the terrorism financing.	None	4.20
		One training course	3.56
		Two training courses	3.83
		Three training courses	4.14
		Four training courses and more	4.94
17	Businesses have awareness and knowledge of the danger of money laundering and the terrorism financing.	None	4.20
		One training course	3.28
		Two training courses	3.17
		Three training courses	4.33
		Four training courses and more	4.94
18	SAFIU provides training programs to fellow government agencies that educate on combating money laundering and terrorism financing.	None	3.80
		One training course	4.22
		Two training courses	4.00
		Three training courses	4.57
		Four training courses and more	4.61
19	SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	One training course	4.39
		Two training courses	4.50
		Three training courses	4.71
		Four training courses and more	4.89

From the table, the researcher identified that SAFIU should operate their offices in major cities confirmed by ascending order of agreement by age groups (Q1, mean 4.29; 4.48; 4.87; 5). This finding was also similar for SAFIU providing guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing (Q2 means 4.32; 4.69; 4.87; 5).

On the question of whether SAFIU receives and reviews STRs that are not related to money laundering and terrorism finance, the distribution of answers were skewed towards neutral by qualification grouping (Q3, mean 3.17; 3.05; 2.93; 4). Based on the overall mean, earlier results indicated that SAFIU should provide more training. Further distribution of answers by qualification highlight that staff with secondary or

less qualification require more training (mean 3.33), including some staff with a bachelor degree (mean 3.89), whereas staff with diploma and masters degree agreed that SAFIU provides sufficient training (Q4; mean 4.48; 4.67). The results also revealed that staff with secondary and less qualification were more neutral or disagreed on question 5 (mean 3.00), neutral or agreed with question 6 (mean 3.67) and agreed on the question 7 (mean 4.17).

The distribution of answers by experience on whether SAFIU provides training programs to financial and non-financial institutions provided a mixed response. The ascending order of agreement mean 3.76; 4.06; 4.60 was observed for staff with experience up to 15 years whereas the mean was lower for staff with experience of 15 years and over (mean 4.17). This was similarly the case for question 9.

The distribution of responses by number of trainings provided interesting results. On the question on whether SAFIU receives and reviews STRs that are not related to money laundering and terrorism finance, staff with more training disagreed with the statement, whereas staff with no training skewed towards agreeing with the statement, highlighting a probable misunderstanding of the question. Further analysis of questions 11 to 19 (due to rising order of responses in terms of mean) indicate that additional training increases awareness and the readiness of SAFIU staff to accomplish their job responsibilities effectively.

4.5. Chapter summary

Overall, the analysis deduced that SAFIU is perceived by respondents to be very effective in the majority of areas investigated. The areas that are perceived by the respondents to be most effective is in maintaining authority to gather the required documents from SAMA and Saudi Arabia Capital Market, classifying STRs according to the suspicious nature and in coordinating the divisions of SAFIU. Effectiveness was also evidenced in accessing financial, administrative and law enforcement information, confiscating property, freezing accounts, exchanging information regarding money laundering and terrorism finance with other domestic government agencies, and in exchanging information with FIUs in other countries through the Egmont Group.

On the other hand, the results highlighted that SAFIU is perceived to be less effective in receiving and reviewing STRs that are not related to money laundering and terrorism financing activities. Further, SAFIU was deemed to be ineffective in providing staff training, allocating sufficient staff, disseminating the latest information on money laundering and terrorism financing activities received from fellow government agencies, and in providing training programs to financial and non-financial institutions. The results also indicated that the MOI needs to provide the necessary financial and technical resources necessary to enhance the performance of SAFIU, and needs to ensure that exchange programs with foreign FIUs occur.

This chapter presented a descriptive statistical analysis for the quantitative and qualitative data collected from the respondents. In the next chapter (Chapter 5: Discussion) the data analysis is explored further to illustrate, discuss and examine the compliance of SAFIU to international standards.

CHAPTER 5: DISCUSSION OF RESULT

5.1. Introduction

The primary goal of this thesis is to examine and investigate the effectiveness of SAFIU in dealing with methods of preventing money laundering and terrorism finance based on the 40+9 FATF Recommendations. The study surveyed SAFIU staff members to gain their opinion on SAFIU's legal framework and its compliance with international AML and CTF standards. A set of results on the effectiveness of SAFIU in the following four areas were yielded:

- Receiving, analysing and administering STRs in combating money laundering and terrorism financing
- Administering activities of combating money laundering and terrorism finance crimes with other governmental and non-governmental agencies, such as financial and banking institutions
- International cooperation between SAFIU and FIUs in other countries in combating money laundering and terrorism finance crimes
- Suggestions to enable SAFIU to formulate policies in combating money laundering and terrorism finance crimes in a better way.

Generally, analysis on the quantitative results indicates that SAFIU is highly effective within the context of the four areas identified. However, there were particular areas in which SAFIU is considered to be less effective. It is important to assess both areas as such an assessment will highlight to SAFIU its strengths and potential areas of improvement. These findings will be valuable for evaluating and assessing the compliance of SAFIU, and subsequently identifying appropriate actions that may create an effective AML and CTF framework. Further, with this type of knowledge, significant recommendations can be made to SAFIU and other entities, and assist in curbing the crimes of money laundering and terrorism finance. This section discusses the quantitative and qualitative results of the respondents, links it to the literature review conducted, and forms the foundation from which the recommendation and conclusion will be derived.

5.2. Q1 –What is the effectiveness of SAFIU in receiving and analysing reports?

One of the purposes of this study is to investigate the effectiveness of SAFIU in receiving and analysing STRs related to money laundering and terrorism financing crimes. Of the 29 questions presented, the quantitative findings as perceived by respondents are that SAFIU is highly effective in receiving and analysing STRs. These findings support the first hypothesis of this study and are discussed further below.

5.2.1. Effectiveness in receiving STRs

SAFIU is highly effective in receiving STRs on suspicious transactions related to money laundering and terrorism financing**.** Feedback from SAFIU staff members confirms that there is strong agreement on the extent of authority given to SAFIU to obtain required information from financial and non-financial institutions. The responses highlighted SAFIU's compliance to FATF Recommendation 26, Article 4, which states that the FIU, either directly or indirectly, should be authorised to obtain information from reporting parties needed to properly undertake its functions. SAFIUs compliance in receiving STRs is also evident through the Egmont Group's definition, which dictates that an FIU is a:

> 'central, national agency responsible for receiving (and, as permitted, requesting), analysing 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 legislation or regulation, in order to counter money laundering and terrorism financing.' (Egmont Group, n.d)

SAFIU staff also confirmed that SAFIU is effective in receiving STRs through various channels of government and non-government bodies (average 4.88). These findings comply with FATF Recommendation 26, Article 4, which is also complimented by Article 11.3(a) of Saudi the AML Law which states that SAFIU is authorised to receive STRs from financial, non-financial institutions and government agencies. Within KSA, supervising authorities are also obligated to this law and include Saudi Arabian Monetary Agency (SAMA), Capital Market Authority (CMA), MOCI, Ministry of Social Affairs (MOSA), MOJ, Ministry of Islamic Affairs

(MOIA) and Saudi Customs. These authorities perform the following supervisory functions:

- SAMA licenses and supervises financial institutions such as banks and money changers
- CMA licenses and supervises securities firms
- MOCI supervises business and corporations according to commercial laws
- MOSA licenses, registers and supervises general charities
- MOIA licenses, registers and supervises education charities
- MOJ supervises the judicial system including lawyers and notaries
- Saudi Customs supervises travellers and goods that enter and leave the KSA.

A similar pattern is also observed in Canada, where FINTRAC through the Proceeds of Crime and Terrorist Finance Act, has the authority to obtain information from other government agencies (Murphy, 2006). It is also consistent with Magnusson's research (2009), which reported that the Swedish FIU receives reports through banks, money exchange agencies, auditors, car dealers, casinos, money remittance agencies, and financial companies. This compliance is also in line with AUSTRAC and FIU_IND who have the legislative power to obtain information from both financial and non-financial bodies. Whilst this was not always the case in Belgium, the law was amended to incorporate reports from non-financial institutions, as they were believed to manipulate the AML legislation. The 2010 MENAFATF report identified the growing trend in STRs reported to SAFIU during the period of 2004 to 2008, and identified the increased reports as a positive development of SAFIUs compliance in receiving STRs. During 2010, SAFIU received a total of 1368 STRs constituting 171 from government agencies, 1137 from finance institutions, 59 from businesses and a single one from non-profit organisations (NPOs) (MOI, 2010).

Results from the questionnaires also reflect a strong agreement of SAFIUs authority to access directly and indirectly the databases of the governmental agencies containing information about suspicious transactions. This finding coincides with the required methods for FATF Recommendation 26, Article 3, which states that FIU's are to have direct or indirect access to administrative and financial information of the government agencies. As direct access to databases of SAMA, MOJ, MOIA, CMA

and MOSA NPO is not granted, SAFIU requests information from the MOCI Corporate, SAMA Registration Database, CMA Securities Information Database, Customs Currency Database, MOJ Real Estate Database and MOSA NPO Database. The authority to access the information from the databases of other government agencies, such as SAMA and MOJ, lies within the Information and Studies Division of SAFIU which plays the vital role of maintaining databases for SAFIU and requesting information exchange from local government bodies. Between 2004-2008, SAFIU disseminated 665 requests for information from other government agencies. Of these requests, 368 were sent to MOCI and SAMA, CMA received 6 requests respectively while the Intelligence Police received 7 requests. The Saudi Customs, which has the authority to investigate such cases, directs incidents of suspicious declarations to SAFIU by enabling a real-time information flow between them.

Having access to databases exponentially increases information processing by presenting SAFIU with opportunities of acquiring and using data to expedite investigations. Gaining database access directly and indirectly is important, as it enables SAFIU to receive fast and comprehensive information thereby reducing STR backlogs and improve decision-making process. This concept is also seen in the UK FIU, SOCA, where it obtains information directly from the databases of TFT and NTFIU. The FIU model in KSA is however different to the UK FIU, who in addition to accessing information from financial institutions is able to monitor real-time information of an account. Monitoring information on a real-time basis is more evident in countries that have implemented the supervisory FIU model enabling them to have direct access to the databases of financial institutions and law enforcement agencies. The importance of utilising databases a mechanism to aid in investigations and prosecution has been recognised in Europe, where the European Union has developed a central interlinked database containing cross border STRs (Stefanou, 2010).

There is a strong agreement among SAFIU staff that SAFIU is authorised to request additional information from financial and non-financial institutions needed to carry out actions to counter money laundering and terrorism financing. This finding is consistent with FATF Recommendation 26, Article 4, which states that FIU should be authorised to obtain additional information directly or indirectly from the reporting

parties. Compliance to this recommendation is evident in Article 11.3(c) of the Saudi AML Law which stipulates that SAFIU has the authority to request additional information from the relevant supervisory authorities, such as SAMA, CMA, MOIA, MOCI and MOJ. Concerning the database, SAFIU staff members strongly agreed that SAFIU has established a database that contains information received and captured from incoming STRs. These findings are in compliance with Article 11.3(b), of the Saudi AML Law, which stipulates it is to develop a database containing all reports regarding suspicious transactions. In response to this law, the Information and Studies Division of SAFIU has developed an internally interlinked database that caters for received, analysed and disseminated STRs. This ease and accessibility of utilising such a database enables SAFIU to exercise it authority in resolving STRs efficiently. Similar compliance was evidenced in Germany, where a database containing all STRs received was inaugurated once the FIU was opened.

There is also an agreement among SAFIU staff that SAFIU has a secure database of all received reports on suspicious transactions related to money laundering and terrorist financing crimes. This is in compliance with FATF Recommendation 26 Article 7, which requires FIUs to develop securely protected databases that contain reports and information related to money laundering and terrorism finance. The servers within SAFIU are located securely within their premises and managed by their Information Technology Division. These servers are considered secure as they cannot be accessed and approached without appropriate clearance authorisation. In line with securing the database, information maintains identity confidentiality as per FATF Recommendation 14, Articles 2 and 3, which emphasises that confidentiality of individuals who provide information to FIUs must be maintained. This recommendation is further highlighted by Article 25 of the Saudi AML Law and Articles 12.4(d) and 13.2 of SAMA AML and CTF, which set out the legislative requirement to ensure that individuals who report suspicious transactions are protected from liability. SAFIU staff indicated a strong agreement to this compliance, and highlighted that the SAFIU policies in place do not conflict with confidentiality and cannot be used against them in the case of any criminal proceedings. Such Laws are consistent with the UK judicial system, which also ensures protection of individuals who provide information to FIUs. Ensuring confidentiality of information

providers increase the flow of information to and from financial units, and contributes to improving work performance within SAFIU.

The feedback from SAFIU staff reflects their strong agreement that SAFIU utilises and benefits from the STRs stored in the database. In addition to receiving and analysing STRs, the Information Gathering and Analysis Division of SAFIU is also responsible for archiving STRs for future research and analysis. This information stored in databases is utilised to pursue detecting typologies, in drafting policy solutions and also provides information when requested by foreign FIUs. Similarly, the FIU in UK, SOCA, maintains the Elmer database, which is utilised by the NTFIU to review and analyse historic SARs stored when searching for information on the existing suspects. Utilising existing information on historic STRs benefits FIUs by enabling analysis and pattern development to be provided when investigating current cases.

Feedback received from the respondents strongly indicates that a compensation mechanism is in place for individuals who provide information related to suspicious activities. In 2003,, SAFIU announced a reward package with prize money ranging from US$270,000 to US$1.87 million for any individual providing information that leads to a suspect's arrest or prevention of money laundering and terrorism activities (Prados & Blanchard, 2004). Rewarding informers is evident in other countries such as Nigeria, where rewards are provided to individuals who assist the FIU in providing information related to money laundering and terrorism finance as financial appreciation encourages individuals to be more disclosing.

A strong agreement was also evident in SAFIU when reviewing STRs received for completeness. The high result (average of 4.34) indicates the implementation of SAFIU in fulfilling its responsibilities of validating all STRs received for compliance and completeness. Within SAFIU, the Reports Division is accountable for receiving STRs and verifying them for completeness and is charged with supporting the Article 7.3 of the Saudi AML Law, which requires reporting entities to complete forms that include personal, transactional, reasons for suspicion and relevant account information. In the case of financial institutions, reporting entities must provide copies of account details, including statements for the last six months and any other

supporting documents related to the nature of the suspicion. Non-financial institutions on the other hand provide information that encompasses business statements and transactions. Both financial and non-financial institutions submitting the initial STR have 10 working days to provide additional information in support of the STR. SAFIU staff members review such requirements and ensure that STRs completed contain this information.

An agreement was received from staff members that SAFIU uses a standardised form that captures all the required information when receiving STRs. A standardised form is required to comply with FATF Recommendation 26 Article 2, which states that FIUs are to provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures that should be followed when reporting. SAFIU utilises four different standardised forms for financial, non-financial, individual and private entities to report to SAFIU once suspicious transactions are discovered. In addition, reporting entities are also provided with a guidance manual that contains information about reporting obligations and typologies, reporting style and explanation of forms (MENAFATF 2010). Using standardised forms to capture disclosed information is also evident in FIU_IND, AUSTRAC and German FIU where the standardised forms lead to greater consistency of data captured.

Respondents also agreed that SAFIU gathers information not only relating to individuals, but also suspicious companies involved in money laundering and terrorism financing. An example of this is with NPOs, such as charities which SAFIU supervises in conjunction with MOSA and MOIA. Further, information about stock exchange companies is gathered through their AML units in the CMA, which is part of the MOJ. Such compliance is in accordance to Article 8.1 and 8.2 of the Saudi AML Law, which outlines that information from financial and non-financial institutions is provided by the relevant agency upon request by SAFIU. One of the private charitable societies, Al-Haramain Islamic Foundation was monitored as it was determined that the Somalian and Bosnian branches were involved in terrorist activities with the Al-Itihaad-al-Islamiya organisation. Accounts belonging to these branches were seized, and a warning order was sent to all charities within KSA to suspend their interaction until further notice (Cordesman, 2003). Most of the Acts,

such as the 2001 Anti-Money Laundering Act (AMLA) of Malaysia, mandate the identification of suspicious companies to money laundering offences by collecting information about suspicious companies and institutions thereby ensuring that any person who utilises companies to engage in illegal activities are investigated and brought to justice.

In reviewing the results of the number of SAFIU staff allocated to the volume of reports received, 71 per cent of SAFIU staff agreed on this notion, 8 per cent were neutral while 21 per cent disagreed. SAFIU currently has only 11 staff in their Reports Division who operate on a 24/7 shift. These findings are consistent with the 2010 MENAFATF Mutual Evaluation Report, which highlighted 20 vacancies across SAFIU. This finding does not comply with Recommendation 30, Article 1, which highlights that FIUs should be sufficiently staffed to perform their functions effectively. It is important to note, however, that resourcing constraints are not specific to SAFIU as the Swedish FIU; NFIS is facing similar problems, where there is a shortage of staff in handling STRs and initiating information for trials. The number of reports over the years has increased drastically, and it was challenging to handle the extensive information contained in the received reports. It was also observed that the types of crimes in those trial cases turned out to be frauds and tax crimes, and only a few were related to money laundering. Within SAFIU, 350 STRs were received in 2004 by the Reports Division and this has significantly increased to 1,368 STRs in 2010 (MOI, 2010), highlighting the need to increase staff members within this area.

Neutral results were also evident in SAFIU receiving and reviewing STRs not related to money laundering and terrorism financing. This demonstrates insufficient efforts by SAFIU in analysing reports that are not related to money laundering and terrorism financing crimes. This could be due to the legal framework of SAFIU, which lists one of the institutional duties and powers of SAFIU as receiving suspicious reports related to money laundering and terrorism finance activities only. These results however, are in compliance with Recommendation 13 Article 1 and Recommendation 6 Article 1 of FATF that articulates that a financial body is obligated to report STRs only if there is a reasonable ground of suspicion that funds are believed to be the proceeds of money laundering and terrorism financing. The results from the respondents was also

identified in the 2010 MENAFATF report, which highlighted that receiving STRs not related to money laundering and terrorism finance is attributed to the reporting body's lack of clear distinction between STR identification and transaction monitoring. This was evident in the number of STRs received in 2010 as being 1368 of which only 526 were forwarded to other authorities for further investigation (MOI, 2010). Magnusson (2009) has observed a similar pattern in Sweden, where exchange offices were reporting every transaction above 15000 Euros to NFIS without any verifying whether these transactions are related to money laundering and terrorism finance offences.

In summary, SAFIU is generally perceived as effective in receiving STRs, particularly in the areas of receiving STRs through various channels by accessing databases of other governmental agencies. SAFIU was also perceived to be effective in areas such as maintaining confidentiality of information providers, investigating received reports related to suspicious transactions and gathering information on suspicious companies. SAFIU staff also agreed that in accordance with Saudi AML Law, SAFIU has the authority to request information on financial and non-financial institutions from the supervisory bodies, such as SAMA, CMA, MOSA, MOJ and MOCA. SAFIU staff however, were mostly neutral on the notion that staff allocated towards receiving STRs were sufficient.

5.2.2. Effectiveness in analysing STRs

From the results obtained, SAFIU is regarded as being highly effective in analysing reports on suspicious transactions related to money laundering and terrorism financing crimes. In accordance with FATF Recommendation 26, Article 1 states that FIUs should act as a national centre for receiving, analysing and disseminating STRs concerning money laundering and terrorism finance activities. Although SAFIU in general is perceived as being effective in analysing STRs, specific areas as discussed below require further improvement.

A large number of SAFIU staff members strongly agreed that SAFIU analyses STRs on money laundering and terrorism financing based on the nature of suspicion (average 4.97). Analysis of these reports are handled by the Information and Studies Division of SAFIU which performs the role of registering, performing initial analysis and adding information contained in the databases of SAFIU and other government

agencies. Once completed, the reports are passed to the Evaluation Committee which determines whether the Information Gathering and Analysis Division will take up the report prior to sending the reports to investigation authorities (MENAFATF, 2010). This step is deemed important, as it assists experts to investigate crimes according to their specialised field. This approach is practiced in Belgium, where a committee verifies the nature, legitimacy and gravity of suspicious transactions prior to commencing investigations (Verhage, 2009). Further, the suspicious transaction is also categorised as to whether it is related to money laundering or terrorism financing, as different skills sets are required in each instance. The responses from SAFIU staff also highlight the existence of coordination in analysing STRs between legal and financial specialists (average of 4.92). Legal personnel provide skill sets for tracking legal and anti-corruption cases while financial staff contributes to analysing financial data. Collectively, both function as watchdogs within the analysis phase as they form part of the evaluation committee that validates STRs received and approves them for further investigations. This functional performance is supported by Recommendation 30, Article 1 of FATF, which outlines the need for skilled staff to be provisioned with technical resources that enable them to perform their functions fully and effectively.

In terms of SAFIU's authority to obtain personal information from financial institutions, SAFIU staff provided feedback that suggests its high effectiveness in this particular area (an average of 4.89). This is in direct correlation to FATF Recommendation 26, Article 3, which indicates that FIUs are to gain access to the financial institutions directly or indirectly. Within the KSA, any financial institution related requests are channelled through their supervisory authority SAMA, which obligates them to comply or face heavily imposed fines. Between 2005 and 2009, SAMA imposed fines on 44 banks and money exchange institutions for non-compliance with AML and CTF regulations (MENAFATF, 2010). This process ensures that the flow of confidential information is maintained and controlled by SAMA as dictated by the law since obtaining personal information directly conflicts with secrecy and privacy laws that may deny access to financial information. In fulfilling the AML and CTF obligations, SAMA developed the Rules for Banks and Money Exchangers (RBME) that stipulate basic operational guidelines, rules governing the opening of bank accounts in the KSA, adoption of Know Your Customer (KYC) standards and customer risk assessment. Of significant note is

Article 2.6 of the RBME, which prescribes that all financial information exchange has to be conducted through SAMA, thereby ensuring a controlled flow of confidential information. Based on such legislative procedures, SAFIU adheres to the legal requirements of information exchange and works collaboratively with other government agencies to access restricted and undisclosed information. Countries such as Malaysia provide exemptions for cases specific to money laundering and terrorism finance, where special powers are entrusted to the FIU to enable them to investigate such affairs without breaking the privacy laws.

SAFIU was also deemed effective in employing highly skilled supervisors in analysing STRs (an average of 4.88). This finding is consistent with FATF Recommendation 30, Articles 1 and 2, which stipulate that FIU supervisors be competent and proficient. Supervisors at SAFIU possess specialist backgrounds in finance, policing, law and border control. Technical supervisors are also hired as part of ensuring security frameworks with SAFIU are maintained at a high level. This is evident in the Chinese FIU, JFIU, where designated supervisors are hired as part of the AML process to ensure that staff are processing STRs according to the law and within specified timeframes. In Belgium and the UK, a myriad of experts are also hired by the FIUs to provide specialist advice and supervise issues specific to money laundering and terrorism financing.

It was also evident that SAFIU is effective in recruiting a range of experts from different specialities (average 4.22). SAMA played an instrumental role of providing their financial experts to SAFIU during their early operational stages and assisted SAFIU in developing a broader expertise in financial analysts (MENAFATF, 2010). Similarly, the Evaluation Committee, which determines whether reports are forwarded to investigation authorities, comprises of intelligence, legal and financial experts. Recruiting from a range of accounting, financial, security and legal specialists also complies with Article 11.2 of the Saudi AML, which states that SAFIU recruits specialists and experts from a range of skills to combat money laundering and terrorism financing. Other FIUs, such as Bulgaria, implement similar tactics of employing experts from various departments such as finance and police.

The feedback from SAFIU staff strongly showed their agreement when it came to analysing suspicious companies and institutions (average of 4.55). Since 2003, institutions are obliged to send their STRs directly to SAFIU for further analysis. NPOs, such as charities, are required to report suspicious transactions to their licensing agencies of MOSA and MOIA, who in turn report these transactions to SAFIU. Analysing suspicious companies is vital, as the Egmont Group identified a growing trend of utilising fictitious or shell companies to camouflage and transfer illegal funds. This finding is consistent with that of the Canadian FIU, FINTRAC and SOCA in the UK, who also conduct analysis of suspicious reports received from institutions and provides them to law enforcement agencies. SOCA has also adopted a 'net worth' investigation approach that provides exhaustive information to assist investigators in analysing SARs. This approach leads to the detection of patterns by collecting interrelated facts (Kennedy 2007).

In terms of sufficient staff allocated to analysing reports, more than 70 per cent of the respondents agreed that SAFIU has ample staff in their Information Gathering and Analysis Division (average 3.73). These results were reinforced by the 2010 MENAFATF Report, which indicated SAFIU as having 42 staff members allocated to analysing reports. Conversely, around nine per cent of the respondents indicated neutrality while another 21 per cent indicated that the Analysis Division was short staffed. It is important to note the impact that resourcing has on an FIU and the ability of an FIU to function efficiently as an AML agency. FIUs, such as FIU_IND and the Nigerian FIU, NFIU, have experienced trends of being under resourced.

In summary, SAFIU staff perceived that SAFIU was effective in analysing STRs. In particular, SAFIU was perceived to be highly effective in analysing information between security and financial specialists, obtaining personal information from the banks regardless of privacy laws, employing highly skilled supervisors in analysing STRs, analysing information on suspicious companies and institutions and recruiting experts. SAFIU, however, was less effective in performing analyses appropriate to the volume of reports received.

5.2.3. Effectiveness in managing STRs

The overall average opinion of SAFIU in managing STRs is 4.51 and reflects a strong agreement among staff members. Findings correspond to the FATF Recommendation 26 Article 1, which states that countries are to establish an FIU as a national centre to manage STRs and other information related to money laundering and terrorism financing.

In terms of the coordination of SAFIU divisions, the response received from SAFIU staff suggests that they perceive SAFIU to be highly effective in this area (an average of 4.97). SAFIU collectively consists of seven divisions - four main divisions and three support divisions. Main divisions include Reporting Division, Information Gathering and Analysis Division, Information Exchange and Follow-up Division and Information and Studies division while support divisions include Information Technology Division, Training Division and Financial and Administrative Division. All STRs received by the Reports Division are registered with a reference number followed by a check for completeness. The STR and any supporting documents are then stored electronically by the Information and Studies Division, which performs an initial analysis prior to adding existing information from the SAFIU and other government databases. Once complete, these files are forwarded to the Information Gathering and Analysis Division via the Information and Studies Division for approval from the Evaluation Committee. The Information Gathering and Analysis Division is entrusted with the responsibility of analysing the reports that are suspicious prior to forwarding them to investigative agencies or archiving STRs. Lastly, the Information Exchange and Follow-up Division has the responsibility of ensuring domestic and international cooperation. In terms of support divisions, the Information Technology Division is entrusted with providing technical services to the whole unit, while the Training Division is primarily responsible organising, delivering and developing internal and external courses. Finally, the Financial and Administrative Division provides the supporting framework to enable to SAFIU to fulfil its operative requirements (MENAFATF, 2010).

Feedback from SAFIU staff strongly supports the notion that SAFIU benefits from research and case studies in developing action plans for its departments (an average of

4.92). This responsibility falls within the Information and Studies Division, which is in charge of maintaining all information related to receiving, analysing and disseminating STRs. This section documents information on existing STRs, current convictions and information received from foreign FIUs. Further, this Division is also responsible for following up on current money laundering and terrorism finance issues, trends and patterns. This information is then amalgamated to assist SAFIU in developing typologies that expand on existing policies and procedures. Aggravated information is also utilised to illustrate its performance through annual reporting requirements. The importance of such measures are illustrated by the World Bank and IMF who recommend that FIUs and law enforcement agencies study the complexities in order to find suitable AML and CTF solutions (2004). FATF has also actively conducted assessment programmes in the research, financial and training sector to enable awareness of case studies through educational forums and publications.

In terms of securely archiving information, SAFIU staff members strongly agreed to the compliance with Article 11.3(f) of the Saudi AML Law, which states that SAFIU archives information related to terrorist financing and money laundering. SAFIU servers are securely based at their premises, where the databases have restricted access. Only authorised persons who have undergone appropriate clearance and authority checks have access. The maintenance of database and its files securely resides with the Information and Studies Division (MENAFATF, 2010). With consideration to other FIUs, FINTRAC also secures information received from various federal government agencies in accordance with an agreement under Subsection 66(1) of the Proceeds of Crime (ML/TF) Act (Murphy 2006).

In terms of conducting field investigations, the feedback from SAFIU staff indicates a strong agreement that SAFIU is highly effective in this area (average of 4.45). Conducting field investigations are mainly targeted towards suspicious companies and institutions. This is in accordance with Article 11.3 (g) of the Saudi AML Law, which states that SAFIU has the authority to conduct field investigations and formulate reports that provide information for further investigation by relevant law enforcement authorities. Between 2004 and 2008, SAFIU received 2968 STRs of which 2747 were related to money laundering, while 221 to terrorism finance or related cases. Of all the STRs received, 495 cases were disseminated to investigation authorities as a majority

of the STRs were from banks, exchange offices and other government agencies (MENAFATF, 2010). For field investigations, the agencies responsible are the Anti-drugs Directorate, Public Security Directorate and Intelligence Police, all which reside with the MOI. Internationally, Germany established a special framework, SPITAL, primarily to investigate money laundering and corruption cases involving elite government officials (FIU Germany 2004).

In other areas, such as updating SAFIU staff on new methods of money laundering and terrorism finance crimes, the feedback from SAFIU staff suggests that SAFIU is highly effective in this particular area (average of 4.30). This requirement is in compliance of Article 11.4 of the Saudi AML Law, which states that SAFIU is to keep staff apprised on the latest money laundering and terrorism financing developments. SAFIU, via the Information and Studies Division also actively participates in awareness programs concerning money laundering and terrorism finance offences by coordinating activities with the Permanent Committee. In 2009, SAFIU issued a staff training manual that includes information about money laundering and terrorism finance methodologies and trends, indicators, investigation and analysis techniques, roles and responsibilities, performance outcomes and system operations. Case studies were also included for better understanding of AML and CTF procedures (MOI, 2010). Internationally, the Australian FIU, AUSTRAC has applied several measures to upgrade the skills of their staff and distributed handbooks detailing performance management, job evaluation and training courses. Similarly, the Caribbean FIUs have frequently organised seminars to create awareness about the latest trends in money laundering crimes among the participating nations. Such measures are used to deliver training and education programs as well as informing staff members on current money laundering and terrorism finance trends.

The responses received from SAFIU staff indicate a strong agreement that SAFIU via SAMA is carefully monitoring financial transactions of suspicious and fictitious companies (average of 4.30). This is according to Article 11.3(j) of the Saudi AML Law, which speculates that SAFIU has the authority to coordinate with other authorities charged with monitoring financial and non-financial institutions. The Banking Department at SAMA has developed a series of systems for monitoring financial transactions. The Saudi Arabian Riyal Inter-bank Express (SARIE) for

example is a high-speed payment settlement system, which is connected to all the banks within the KSA. Saudi Payments Networks (SPAN) is another such network, which focuses on connecting all Automated Teller Machines (ATM) and Point of Sale (POS) terminals to a central system. The implementation of such systems enables SAMA to provide requested information on financial transactions of suspicious companies as seen in 2008, where 1306 requests were provided to SAFIU for further investigation (MENAFATF, 2010). In considering other AML organisations around the globe, FinCEN practiced a Belgian-based monitoring system called SWIFT to monitor millions of transactions between stock exchanges, banks and exchanges. The US Treasury Department, CIA and FBI also use SWIFT to monitor transactions and track terrorist outfits nationally and internationally (Bowers, 2009).

While a majority of the respondents agreed that SAFIU organises additional training, 5.41 per cent of SAFIU staff responded neutrally, while the remaining 14.86 per cent disagreed. The importance of FIU training is evident in FATF Recommendation 30 Article 3, which states that FIU staffs are to be provided with appropriate and on-going training that combats money laundering and terrorism financing activities. In compliance of this Recommendation, the Training Division at SAFIU was established to accommodate the training needs of staff and augment their existing expertise. This area in collaboration with Naif University for Security Sciences, Institute of Banking in SAMA and King Fahad Security College specialise in providing training courses in AML, CTF and general systems and analysis training. Training is also carried out to improve the knowledge as to how different systems and business entities can be abused for money laundering and terrorism finance purposes. Further, this Division of SAFIU also coordinates training courses to external entities, such as government and non-government organisations. During the period of 2005 to 2008, a total of 343 training courses were conducted by SAFIU (MENAFATF, 2010). While there is no minimum number of courses that has been set by FATF, the number of courses provided by SAFIU was minimal when compared to other FIUs like the UAE FIU, (AMLSCU), which was noted by IMF as conducting 360 seminars between 2004 and 2008 (IMF 2008).

Overall, SAFIU was perceived by its staff to be highly effective in most of the areas regarding managing STRs. For example, SAFIU was perceived to be effective in

coordinating SAFIU divisions, developing action plans for its departments, archiving received information, conducting field investigations, updating SAFIU staff on new methods of money laundering and terrorism finance crime and receiving financial transactions of suspicious and fictitious companies. SAFIU however was perceived to be less effective in conducting additional training for its staff.

5.2.4. Discussion of qualitative results

Some of the staff comments indicated that SAFIU should introduce electronic systems to receive STRs from reporting bodies. SAFIU currently receives STRs mainly through facsimile, post and by hand delivery. Receiving STRs electronically will not only fasten the receiving process but will also reduce handling errors when inputting information into the SAFIU database. Further, utilising electronic systems to receive STRs ensures that information is efficiently acquired and in a secure manner. SOCA for example receives STRs electronically by utilising 'SAR ONLINE' submission facilities. SAR Online is the preferred way as it only requires internet access thereby facilitating accessibility 24 hours a day, seven days a week (SOCA, 2011).

Some of the SAFIU staff also commented on the ineffectiveness of SAFIU in analysing STRs that are not connected to money laundering and terrorism financing. As these are not considered part of its core function, such STRs are not analysed but are archived into a database prior to being sent to other authorities. SAFIU for example forwarded 117 non-money laundering and terrorism finance cases to other supervising authorities between 2004 and 2008: 97 to the Public Security Directorate, seven to MOCI, three to SAMA and 10 to other entities (MENAFATF, 2010). A similar pattern is also observed in the Swiss FIU, which focuses only on STRs linked to money laundering and terrorism financing. This contradicts with the draft Article 4b of the UN Convention against Transnational Organized Crime, which states that FIUs should not only serve as agencies analysing and disseminating STRs related to money laundering, but also as national centres for investigating other forms of financial crimes (cited in Mitsilegas 1999, p.157). The complexity however is due to FATF Recommendation 26, which states that FIUs are to act as national centres which receive, analyse and disseminate reports on money laundering and terrorism finance activities. Further, the KSA Law grants each agency a specialist area of focus as seen with MOI, MOCI, Customs and MOJ, and provides clear regulations on each

areas responsibilities thereby ensuring that each agency has its own authority and autonomy to administer its roles. As such, SAFIU is only able to focus on being an agency that analyses money laundering and terrorism financing related STRs.

Respondents also highlighted that some of the financial (non-banks) do not adhere to reporting procedures. The shortcoming is credited to their staff's lack of experience and training on money laundering and terrorism financing activities. Delays in providing supporting information hinder SAFIUs ability to commence its analysis and investigations. Further, a few respondents indicated that a lack of understanding on the parameters by reporting bodies that constitute monitoring and reporting an STR. These shortcomings are due to SAMA being the supervisory authority for financial (non-bank) institutions, such as money changers and insurance companies, and holds the responsibility of the clarifying the AML and CTF rules and regulations for these institutions.

5.3. Q2 – What is the effectiveness of SAFIU in administering activities with government and non-government institutions?

Another purpose of this study is to investigate the effectiveness of SAFIU in administering activities with government and non-government institutions. Of the 27 questions presented, the quantitative findings as perceived by staff members are that SAFIU is highly effective in this area. These findings support the second objective of this study and are discussed further to identify whether SAFIU complies with the international standards as set by FATF.

5.3.1. Effectiveness in administering activities

The feedback provided by the SAFIU staff reflects their agreement that SAFIU has direct access to the law enforcement information on a regular basis (average of 5.0). This is in consistence with FATF Recommendation 26 Article 3, which grants FIUs with the power to administer law enforcement information from authorities. SAFIU has direct access to the domestic law enforcement database known as the National Information Centre which is maintained by MOI. This database contains information from the policing, immigration, traffic and drugs departments and holds identification information, such as birth certificate, passport, car registration, of both citizens and

foreigners. In addition, the law enforcement database includes a list of criminals and their previous convictions.

In terms of the SAFIU's authority to request authority to freeze accounts and confiscate properties used in activities related to money laundering and terrorism financing, the feedback from SAFIU staff indicates that they perceive SAFIU as highly effective scoring an average of 5.0. This is in line with FATF Recommendation 3 Article 1, which states that every nation is to have legislative power to confiscate properties derived from the proceeds of such crimes. This is also validated by FATF Recommendation 3.2, which states that every country should have effective laws and procedures to freeze funds or assets believed to be proceeds of terrorism activities. Within KSA, Article 12 of the Saudi AML Law asserts SAFIU as the authoritative body that requests the prosecuting authority to carry out preventive seizure of properties and funds associated with terrorism financing and money laundering crimes. SAFIU exercised this authority four times in 2006 whereas in 2008, three cases required this law to be enforced (MENAFATF, 2010). This finding is also consistent other FIUs, such as SOCA, which utilises the 2008 Counter Terrorism Act to freeze the assets of persons or companies believed to be connected with acts of money laundering and terrorism. Similarly, the Malaysian FIU, UPWBNM also has the authority to freeze funds and assets involved in terrorism financing.

When analysing whether the roles and responsibilities of reporting bodies that deal with SAFIU are clear and specific, the feedback indicates a strong agreement that this is the case. SAMA is the supervising and regulatory authority for banking sector that controls and issues currency manages foreign currency and regulates money supply. SAMA additionally undertakes supervision of money exchange and transfer businesses while MOCI and the MOF caary out the licensing role. PCCML which comprises of members from the MOI, SAMA, SAFIU, MOJ, MOCI, MOF, MOFA, CMA, Customs and Prosecution Authority departments is responsible for AML and CTF policy coordination and FATF standards implementation.

With consideration to the right of SAFIU to disclose financial information to local authorities, the feedback provided by the SAFIU staff evidenced a strong agreement

that SAFIU is highly effective in this area (average of 4.96). This indicates compliance with FATF Recommendation 26 Article 5, which states that FIUs should be authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect money laundering or terrorism finance related activities. Observance of this recommendation was evident in 2009 to 2010, where SAFIU disseminated 1288 out 2598 STRs for further investigation to other authorities (MOI, 2010). Internationally, the Australian, Canadian, Brazilian and Bulgarian FIU have opted for an Administrative Model, where the FIU uses its authority in centralising information and subsequently passing it to the concerned law enforcement agencies. SAFIU, on the other hand, utilises the Law Enforcement Model where it liaises with existing law enforcement agencies. The drawback of this model is that SAFIU, at times has to compete for jurisdictional authority for money laundering investigations (Masciandaro, 2005). The Chinese FIU, JFIU has also adopted the Law Enforcement Model, and allows the FIU to disclose financial information to law authorities for investigation and necessary legal actions.

Other areas that were explored by the study included the availability of secured networks and communication channels between SAFIU and governmental and non-governmental institutions. This is to ensure compliance to FATF Recommendation 40 Article 2, which states that FIUs are to possess strong operative gateways that facilitate immediate information exchange between concerned parties. According to the findings, SAFIU staff strongly agreed with the availability of secure network and communication channels between SAFIU, governmental and non-governmental institutions (average of 4.91). Within SAFIU, the Information Technology Sub-division is responsible for securing the network and covers three main aspects of information technology: System Analysis, Information Security and Technical Support. The System Analysis section is charged with ensuring that the systems mounted are technically capable of satisfying SAFIUs secure requirements, while the Technical Support section safeguards telecommunications and computer systems by securing SAFIUs communication network. Finally, the Information Security section applies relevant methods to safeguard the centre's information and by monitoring the network (MOI, 2011). This type of network ensures that information exchanged between SAFIU, government and non-government agencies is effective and secure. In China, JFIU also utilises secure networks that captures information about suspicious

transactions in finance, government, banking and non-banking sectors. Availability of secure communication channels between FIUs and their supporting agencies increase the flexibility of information disclosure and enhance the simplicity and the rapidness of the circulation of money laundering and terrorism finance information.

According to the respondents, SAFIU is perceived as highly effective in tracking and freezing accounts through the Prosecution Authority (average of 4.84) in accordance with FATF Recommendation 3 Articles 2 and 4, which states that laws should accommodate measures for tracing and freezing of property and accounts that may be subject to confiscation. The 'Rose Garden Strategy' complements this recommendation, asserting that countries are to freeze assets or funds believed to be supporting terrorist activities. Within the KSA, Article 12 of the Saudi AML Law provides SAFIU with the power to trace and identify property involved in money laundering and terrorism finance. This law also outlines provisional measures that enable SAFIU to request the prosecution authorities to seize or freeze funds for an initial period of up to 20 days. Such authority is also evident in the Philippines, where the AMLC has the right to freeze a property for up to 20 days. This is in contrast to the Barbados FIU, which has the authority to freeze a bank account for a period of only five days.

In relation to SAFIU publishing periodic reports, such as statistics, samples, models and objectives and other SAFIU activities, the feedback provided indicates that SAFIU is effective in this area (an average of 4.57). This is an indication of SAFIU's compliance with FATF Recommendation 26 Article 8, which requires FIUs to release periodic reports that include statistics, typologies and trends regarding its activities. SAFIU's annual report is published on the MOI website, and includes performance statistics, operational activities and key efforts of SAFIU. The publication of statistics, trends and typologies together with information on its operational activities is evident across majority of the FIUs such as AUSTRAC, FinCEN and the Belgian FIU, Cellule de Traitement des Informations Financières.

SAFIU was also viewed by respondents as being effective in providing directions and guidance to financial and non-financial institutions regarding procedures to be followed (an average of 4.41). Such measures have been placed through FATF

Recommendation 26 Article 2, which requires FIUs to provide guidelines, specifications and procedures to be followed, while reporting STRs. SAFIU has delivered a consolidated guidance manual for AML and CTF that includes methods and actions performed to inform employees of financial and non-financial sectors on ways of identifying and reporting STRs. This manual also contains comprehensive information on terrorism financing, money laundering and the four standardised reporting forms for suspicious transactions. It also highlights the role of SAFIU as a national receiving and analysing and provides guidance on money laundering and terrorism financing operations. This compliance is consistent with other FIUs, such as the Georgian FMS, who also published various guidelines and regulations to create awareness of money laundering procedures among financial and non-financial institutions.

The feedback from SAFIU staff indicates their strong agreement of SAFIU under the supervision of SAMA imposing its control over financial institutions. SAMA is the supervisory authority in regulating and supervising financial institutions for AML and CTF purposes and has additional powers to inspect financial institutions on-site. SAMA for example utilises Regulation 4.1 of Rules Governing AML and CTF, which enacts SAMA as the legal entity that receives STRs from the bank's money laundering control unit. Furthermore, SAMA coordinates with SAFIU on all suspicious cases by instructing banks on guidelines and issuing updates when necessary. SAFIU and SAMA are members of PCCML, which is responsible for coordinating, and ensuring FATF standards in financial institutions are implemented. Article 8, 8.1 and 8.3 of the Saudi AML stipulates that SAFIU can exercise its authority to obtain information from financial institutions through the AML units of other authorities. Financial institutions are obligated to respond to SAFIU requests within a period 10 days. SAFIU's 2010 annual report stated that 862 requests were made by SAFIU to SAMA for financial information with an execution rate of 100 per cent. In addition, imposing control on financial institutions ensures policies related to the combat of money laundering and terrorism financing crimes implemented and are consistence with Article 11 Section 3(j) of the Saudi AML Law. This law provides SAFIU with the right to coordinate, monitor and control departments to ensure compliance of financial institutions. Internationally, the Japanese FIU, JAFIO, in conjunction with the FSA, monitors the compliance of financial institutions according

to AML and CTF. Such controls ensure the compliance of these institutions with SAFIU policies.

The analysis also indicated an agreement by respondents that SAFIU has sufficient freedom and autonomy to perform its operations and is not subject to external influences and interference (average of 4.32). This prerequisite is essential as FATF Recommendation 26 Article 6, requires all FIUs to have adequate operational autonomy and independence and not be subject to interference and undue influence. Despite this agreement, 4.05 per cent of staff was neutral, while 16.22 per cent disagreed. While SAFIU reports to the assistant Minister of Security Affairs at MOI, its budget is separate from MOI and spending is controlled by the head of SAFIU who has the discretionary power to run operational affairs, promote, recruit and grant material incentives. The lack of autonomy arises when dealing with other government agencies such as SAMA, who administer regulations for financial institutions and as such limit the direct influence and freedom. The Saudi AML Law however does dictate that other government agencies are to recognise SAFIUs authority and comply with any requests relating to suspicious transactions, but this is in contrast to other FIUs such as CTIF, where independent legality entitles them to access, analyse and process STRs directly.

In terms of SAFIU's continuous monitoring of money laundering and terrorism finance crimes, the feedback from respondents indicates that staff perceive SAFIU to be highly effective (average of 4.31). This type of monitoring is performed in collaboration with other government agencies, such as SAMA for banks, insurance, financing businesses and exchange businesses and CMA for securities business. This is in compliance with Article 1 of the Saudi AML Law, which designates these agencies as having the supervisory authority to monitor, supervise and license them. The Banking Supervision Department and Banking Inspection Department within SAMA is primarily responsible for off-site and on-site monitoring of banks, financing companies and money exchange, while the Insurance Companies Department is tasked to license and monitor insurance companies. These departments ensure the bank's compliance and provide financial information to SAFIU upon request (MENAFATF, 2010). As MOSA and MOIA are responsible for monitoring and licensing charities, SAFIU has indirect access to the electronic databases of MOSA

and MOIA, which hold information on the charities, their donors and recipients, financial position and quarterly reports. A similar approach is also undertaken in Malaysia, where UPWBNM in conjunction with the National Bank collaborates with another 12 domestic and foreign agencies in monitoring and sharing information. As such, periodic and continuous monitoring of financial and non-financial crimes in collaboration with other government agencies enhances the efficiency of SAFIU in monitoring money laundering and terrorism finance crimes.

Although certain SAFIU respondents indicated an agreement regarding the availability of advanced knowledge and awareness in banking institutions, 4 per cent of staff were neutral, while 16.22 per cent disagreed. This compliance is in response to Recommendation 15 Article 3, of FATF which requires banking institutions to establish training procedures to inform employees of the latest developments on money laundering and terrorism finance techniques, methods and trends. Findings of the MENAFATF 2010 Mutual Evaluation Report questioned the overall number of STRs submitted when compared to the economic size of the country. Further, the report cited a significant number of monetary transactions are undocumented and therefore contribute to the low number of suspicious transactions reported to SAFIU. Over the period of 2004 to 2008, only 2347 STRs were received from banks. A similar outcome was also deduced from businesses, where a high percentage of SAFIU staff (21.62 per cent) highlighted that businesses generally do not have advanced awareness and knowledge on the risks and requirements of combating money laundering and terrorism financing. This is despite Article 7.1 of the Saudi AML Law stipulating that businesses setup indicators for developments in transaction monitoring and also pay special attention to complex transactions. This was consistent with the Mutual Evaluation Report findings, which underlined the importance of an effective system being implemented by the supervisory authorities to examine the AML compliance of business institutions as real estate agents and dealers of precious stones, accountants, lawyers and auditors. The jurisdiction of these entities lies with the SAMA, MOJ and MOCI, as these are the supervisory bodies of financial and non-financial institutions. Despite AML and CTF circulars being disseminated, increased awareness and knowledge is still required (MENAFATF, 2010). This issue was also evident in China, where in 2009, the FIU initiated an AML Strategic Plan to counter against the lack of awareness on the risks of money laundering. In Belgium, non-

financial institutions, such as lawyers and casinos, have gradually adopted AML legislation and are obligated to report suspicious transactions to CTIF. In 2010, a similar approach of implementing a strategy that better cooperates with financial and non-financial institutions to raise their level of awareness in reporting requirements, indicators, training needs, trends and new methods was released by SAFIU (MOI, 2010).

Despite the feedback from certain SAFIU staff indicating their agreement that the PCCML supports the objectives of SAFIU (average of 3.89), 2.70 per cent of staff remained neutral on this notion, while 15.57 per cent disagreed. The PCCML coordinates with SAFIU on the issues concerning money laundering and plays a significant role in leading the Saudi delegation to MENAFATF, FATF and other international bodies. As the PCCML constitutes membership from MOI, SAMA, SAFIU, MOJ, MOCI, MOF, MOFA, CMA, Customs and Prosecution Authority, issues of awareness, training and non-compliance should be raised to ensure that the AML and CTF framework is adhered to. Further, this is the only forum where all members are able to raise concerns, formulate a collective response, and implement strategies that address any compliance shortcomings.

Lastly, the responses indicate agreement with SAFIU disseminating the latest trends on money laundering and terrorism finance crimes to government and non-government agencies (average of 3.85). This is in accordance with FATF Recommendation 26 Article 8, which requires FIUs to release information on a regular basis that includes latest trends and statistics about terrorism financing and money laundering activities. Within the KSA, the PCCML is charged with disseminating the latest information and circulars on money laundering and terrorism finance upon provision from SAFIU. This is to ensure that all supervisory members of the reporting bodies receive the latest trends. SAFIU also maintains a public website, which provides the latest information for the general public. This compliance is in response to the World Bank's requirement to disseminate information on suspicious transactions to various government agencies. This is considered as an integral part of their responsibilities of FIUs (World Bank, 2004). In addition to distributing publications, the Japanese FIU, JAFIO, uses a self-developed database to disseminate

valuable information about money laundering and terrorism financing to law enforcement agencies (Kishima, 2004).

In summary, SAFIU is generally perceived by its staff as highly effective in administering money laundering and terrorism financing activities with other government and non-governmental agencies, such as banking and charity institutions. In particular, SAFIU was perceived to be effective in controlling and commanding activities related to the combat of money laundering and terrorism finance crimes. Other effective areas include SAFIU maintaining direct access to law enforcement information. Further, SAFIU was seen as being effective in freezing accounts and confiscating properties used in activities related to money laundering and terrorism financing crimes. SAFIU however, was perceived to be less effective in providing the FIU with the independence and autonomy to perform its operations. This was also observed in other areas, such as the availability of knowledge and awareness of risks and the requirements for combating money laundering and terrorism financing crimes in financial institutions.

5.3.2. Effectiveness in coordinating activities

The overall opinion of SAFIU staff regarding the effectiveness of SAFIU in coordinating activities related to the combat of money laundering and terrorism financing crimes with governmental and non-governmental is high (average of 4.41).

The analysis confirmed SAFIUs staff strong agreement regarding the exchange of money laundering and terrorism finance information with local government agencies (an average of 4.97). This requirement is in accordance with Article 11, 3(c) of the Saudi AML Law, which states that SAFIU has the authority to exchange and request information from the other authorities by taking required measures in combating terrorist financing and money laundering. The Information Exchange and Follow-up Division of SAFIU is entrusted with the responsibility of exchanging information with the local authorities. In recognising the importance of exchanging activities, China developed the AML Monitor and Analysis Centre (AMLMAC) to strengthen their FIU when working closely with government agencies.

SAFIU staff indicated their strong agreement in the effective coordination of AML units in SAMA, MOCI and MOJ (an average of 4.77). In facilitating the returns of STRs, SAFIU requests these units to provide additional information prior to issuing freezing notices. SAMA issues a listing of identified persons to financial institutions and upon detection, banks freeze the accounts and report outcomes to SAMA and SAFIU. In accordance with Article 1.8, Saudi AML Law only allows SAFIU to request the Prosecution Authority to freeze funds for a period of 20 days on the grounds of suspicion. In addition, Article 12.10 of Saudi AML Law is empowered to apply for the adoption of preventive seizures in compliance with the period specified upon request by the supervisory authorities. Within SAFIU, the Information Gathering and Analysis Division deals with the requests of freezing funds involved in money laundering and terrorism finance activities. Between 2005 and 2008, SAFIU requested SAR800,000 to be confiscated and seized SAR5.5 million money laundering cases. SAFIU also seized 28 cars, 34 mobile phones and 19 computers while SAR71,000 in terrorism finance was confiscated (MENAFATF, 2010).

In terms of SAFIU coordinating with authorities in investigating money laundering and terrorism finance crimes, the feedback from SAFIU staff suggests they perceived SAFIU to be highly effective in this area (an average of 4.69). This is in accordance with FATF Recommendation 31, Article 1 and 8.4.1 which requires FIUs to have effective mechanisms for enabling cooperation and coordination with domestic government and non-government agencies. SAFIU coordinates with the Prosecution Authority, which has the responsibility for prosecuting and referring certain criminal cases to external investigative authorities such as the General Directorate of Investigation and Public Security Directorate within MOI. To ensure proper coordination, the Prosecution Authority has 13 liaison officers in other agencies who, facilitate MOUs for operational cooperation. It also formed bilateral agreements and PCCML membership with non-MOI members such as SAMA and Saudi Customs. These investigative authorities have the responsibility to notify SAFIU and the Prosecution Authority about the developments of cases passed on to them. Between 2004 and 2008, SAFIU coordinated with investigation authorities by disseminating information on 495 cases for investigation purposes (MENAFATF, 2010). SAFIU also coordinated with other government bodies such as SAMA and Saudi Customs on 66 cases for investigative purposes. This finding is similar to the Russian FIU

(FFMS), which coordinates with the Central Bank and other federal bodies in fighting against money laundering.

SAFIU staff expressed their strong agreement with organising regular workshops (average of 4.43) and seminars (an average of 4.39) between SAFIU, government and non-government agencies. In conjunction with SAFIU, MOCI increases awareness of AML and CTF through seminars and conferences conducted in collaboration with the Saudi Chambers of Commerce and Industry. In conjunction with SAFIU, the MOJ has also taken steps clarify AML and CTF measures to legal service providers by conducting a series of annual conferences and seminars (MENAFATF, 2010). The Nepalese FIU conducted a series of workshops involving government and non-government organisations to familiarise them with the concepts of money laundering and terrorist financing crimes. FIUs organising such workshops increase the level of awareness regarding the seriousness of money laundering and terrorism financing crimes, and in turn, assist in developing relationships between organisations attending these workshops. FinCEN has also organised workshops with its allies from Bolivia, Turkey, Ukraine and China. Such programmes are aimed at providing training and technical support to the participating FIU and assisting them to gain operational status by streamlining processes in law enforcement capabilities, legal framework, financial regulatory systems and prosecution (GAO, 2006).

SAFIU staff also strongly agreed that SAFIU was highly effective in providing training programmes that combat money laundering and terrorism finance to government agencies (average of 4.35) and non-government organisations (average 4.12). In accordance with FATF Recommendation 30 Article 3, the Training Division of SAFIU conducts training programs related to money laundering and terrorism finance typologies, investigation and prosecution. As SAMA is the supervisory authority for monitoring and verifying the bank's AML and CTF compliance, it has established a Banking Inspection Department, which specialises in investigating money laundering and terrorism finance crimes. This unit requests SAFIU to train the banking and non-banking companies on the issues and identification process of suspicious transactions. During 2004 to 2008, a total of 4215 bank staff members participated in internal and external training sessions. Similarly, a total 413 participants of non-banking institutions (securities, insurance and financing)

underwent training. Training of 19 Saudi Customs staff and 21 money laundering and terrorism finance training programmes for 339 judges was also provided. Further, SAFIU also trained 117 staff members of the Prosecution Authority on how to investigate money laundering and terrorism finance crimes (MENAFATF, 2010). By organising training programs, SAFIU is familiarising financial institutions with rules and regulations for combating money laundering and terrorism financing crimes. The implementations of such programmes are also evident in the UK, where SOCA liaises with government and financial bodies to provide training and education on combating money laundering. These training courses are conducted to develop a better understanding of the rules and regulations and expand to focus on the current techniques used by money launders. Such activities ensure compliance to the World Bank, which has mandated all staff in financial institutions to undergo training in AML and CTF topologies.

In summary, SAFIU is perceived to be highly effective in most of the areas related to coordinating activities with governmental and non-governmental institutions. SAFIU was seen as particularly effective in exchanging information related to money laundering and terrorism financing with government and non-government agencies. Interestingly, there were no shortcomings regarding SAFIU responsibilities in coordinating these activities with governmental and non-governmental institutions.

5.3.3. Discussion of qualitative results

Some of the SAFIU staff commented on the effectiveness of SAFIU when coordinating with governmental and non-governmental agencies, such as banks and other financial institutions. Their opinions suggested that SAFIU does not issue their annual reports regularly and during a specified time frame. Further, the respondents highlighted that reports would benefit by including additional statistics and models. Additional feedback also indicated that SAFIU should update and improve the current guidance manual provided to financial and non-financial institutions on methods and trends linked to money laundering and terrorism finance crimes.

Comments pertaining to the PCCML indicated that it is supporting SAFIUs role, but not to the desired level. Staff suggested that PCCML has expertise to provide additional indicators to financial and non-financial institutions, thereby enabling them

to distinguish terrorism financing and money laundering transactions better. Further, guidance on typologies would assist the capabilities of reporting entities in identifying suspicious and unusual transactions. Comments received were also related to financial and non-financial institutions lacking skills and knowledge on the requirements for combating money laundering and terrorism finance crimes. Though the number of training programmes and participants has both increased, courses delivered are intensive and can take between one to 20 days.

5.4. Q3 – What is the effectiveness of SAFIU in cooperating with international FIUs ?

The overall opinion of international cooperation between SAFIU and FIUs in other countries is 4.20, indicating a high rate of international cooperation. This supports the third objective of the study and discusses the results as analysed through the 10 survey questions asked.

The feedback from SAFIU staff indicated their strong agreement with the exchange of information between SAFIU and FIUs in other countries through the Egmont Group (an average of 4.93). Recommendation 26 Article 9 of FATF states that every FIU should apply for the Egmont Group membership and SAFIU complied with this recommendation by joining in 2009. This is supported by FATF Recommendation 26 Article 10, which states that countries should have regard to the Egmont Group's principles and statement of purpose, and their FIU should exchange information with other Egmont members. By becoming a member, SAFIU has been able to sign MOUs with fellow Egmont members such as Canada, Germany, UK, USA and Australia thereby facilitating prompt exchange of information. This collaborative approach has also been undertaken by JAFIO who have established collaborations through the Egmont Group with Britain and Belgium.

Within SAFIU, the Information Exchange and Follow-up Division is in charge of exchanging information with the Egmont Group. By utilising the Egmont Secure Web (ESW), SAFIU communicates through the secure network that exchanges money laundering and terrorism finance information with partner FIUs. Using the Egmont Secure Web, SAFIU not only retrieves analytical information, it also acquires updated laws and regulations on money laundering via the network. SAFIU received 80

information requests and requested 54 for investigations related to cases in 2010 (MOI, 2010). Requests received during the same year were significantly lower than Germany, which received 837 requests from foreign FIUs and requested information on 207 cases (Germany, 2010). Additionally, SAFIU staff indicated their agreement about the availability of qualified interpreters in SAFIU to facilitate communication with FIUs in other countries (an average of 4.45). Incoming and outgoing requests through ESW are translated to English as the medium of communication for Saudi agencies is Arabic. SAFIU ensures employees involved in this translation process have a bachelor's degree in English as a minimum, and outlines this requisite when advertising for prospective employees. This approach is similar to AUSTRAC, who utilises translators' accredited by NAATI to counter money laundering crimes. As such, the use of the translators assists in the combating of money laundering and terrorism finance through enhanced communication, coordination and cooperation between FIUs.

SAFIU staff also indicated a strong agreement with the notion that the Saudi AML Law has incorporated clear regulations for international cooperation (average of 4.88). Articles 11 and 22 of the Saudi AML Law gives SAFIU the authority to exchange information with other foreign FIUs based on a valid agreement of reciprocity. SAFIU has shared its information with other FIUs from the USA, Japan, Korea, UK and Germany and the European Union. In 2009, SAFIU processed 10 incoming requests and 43 outgoing requests, while it increased to 80 and 54 respectively in 2010. Further, the KSA since 2004 has signed treaties, multilateral agreements and conventions to facilitate international cooperation of money laundering and terrorism.

Feedback from SAFIU staff also indicated a strong agreement of SAFIU having a database for individuals suspected of international money laundering and terrorism financing crimes (average of 4.57). A special database, known as the Law Enforcement Database, is maintained by MOI and holds information of wanted criminals. In Europe a centralised database promotes better integration and cooperation between various databases. Referred to as the European Union (EU) Database, it was established in Oct 2005 and contains information in standard format, allowing all the member countries to access for prosecutions and joint investigations (Stefanou, 2010).

Other areas that were investigated include the regular participation of SAFIU staff in international money laundering and terrorism finance seminars and conferences. Based on the feedback, SAFIU is perceived to be effective in this area (average of 4.47). In 2005, the capital city of Riyadh hosted the Counter Terrorism International Conference, emphasising the causes of terrorism and validating the link between terrorism financing and money laundering. The conference enabled the 60 participating nations to share experiences, practices and patterns of money laundering and terrorism finance. This year, SAFIU participated in the 13th MENAFATF Plenary in Kuwait, and organised the third MENAFAF Annual Compliance and AML seminar (MENAFATF, 2011). Internationally, the Caribbean FATF (CFATF) has organised seminars jointly with the South American FATF (GAFISUD) and the USA to analyse weaknesses in AML and CTF for the global community by sharing their expertise and knowledge. Participation of SAFIU staff in international seminars and conferences increases their awareness and assists staff in networking and gaining access to latest methods utilised.

Further, SAFIU was perceived as being highly effective in the use of secured communication techniques when exchanging information with FIUs in other countries (average of 4.41). This exchange of information can be accomplished either through Interpol, or the Egmont Group of FIUs. Through ESW and Interpol's I-24/7 global communications network, sharing sensitive and confidential information is conducted through secure chains and restrictive access granted only to a few personnel that have the appropriate clearance levels. KSA coordinates with partner Interpol bureaus around the globe, and receives requests that have a turnaround time of approximately 30 days (Interpol, 2011).

The responses from SAFIU staff indicate their agreement with the exchange of information between SAFIU and FIUs before joining Egmont Group (an average of 4.15). Prior to becoming an Egmont Group member, the Permanent AML Committee dictated that all incoming requests from other countries be channelled either through Interpol or formal diplomatic channels. The MOI executed all international treaties and supervised communications with security of counterpart nations via Interpol. SAFIU exchanged information with Egypt, Senegal, UAE and Bahrain through

Interpol prior to gaining access to the EWS. Incoming and outgoing requests through Interpol during 2005 to 2009 was 62 and 16 respectively (MENAFATF, 2010).

In relation to SAMA exchanging information with their foreign counterparts through SAFIU, SAFIU staff members were neutral on this notion (average of 3.39), indicating a shortcoming of FATF Recommendation 40 Article 2, which states that there should be effective and clear channels or mechanisms that facilitate information exchange directly with their foreign counterparts. As these mechanisms are accomplished through bilateral agreements, MOUs and Interpol, SAFIU staff also strongly felt that there were no safeguards and legal controls to ensure supervisory bodies, such as SAMA and CMA, utilise this information in a lawful manner. SAMA exchanges and cooperates with other central banks through its membership with the IMF, Arab Monetary Fund, World Bank and GCC. If information exchange occurs through SAFIU, then Article 22 of Saudi AML Law, which details of the legal obligations of information exchange by reciprocity, is applicable.

Staff responses were also collected when responding to organising regular visits by SAFIU staff to FIUs in other countries to gain an understanding of effective policies applied in these countries. Most SAFIU staff were either neutral or disagreed with this notion (average of 3.39), suggesting that the number of visits made by SAFIU staff to FIUs in other countries was insufficient. SAFIU for example received a four person team from FinCEN in the first quarter of 2006 for an on-site assessment, while in 2010, SAFIU organised staff visits to FIUs in the USA and Australia and received FIU staff from Germany, Japan, Canada, UK, Senegal and Korea (MENAFATF, 2010). These types of visits provide an opportunity to the participating FIUs to assess their performances and gain practical knowledge in order to further develop their individual performances. AUSTRAC has similarly implemented the Australia-Indonesia project for cooperation, where visits occur to assess performance and gain knowledge (Sathye & Patel 2007).

In conducting regular meetings between SAFIU staff and staff members of FIUs in other countries, the feedback from SAFIU staff indicated that the majority were neutral, while the rest disagreed (average of 3.39). As such, the results indicate a lack of regular meetings as desired between SAFIU staff and staff of investigation units in

other countries. While this is not an international standard, FAFT publications highlight that conducting regular meetings and conducting on-site visits provide an opportunity to discuss the effectiveness of policies. Such meetings also highlight the prospects of accessing the AML criteria of the visiting country, compare it to the host country to provide an opportunity of understanding emerging trends and improve their AML framework.

In summary, SAFIU was generally perceived to be effective when cooperating internationally with other FIUs. SAFIU was deemed as highly effective in exchanging information with FIUs in other countries, in tracking money laundering and terrorism financing and in maintaining an international database for suspects. A number of areas however identified SAFIU as being less effective specifically in relation to programmes through which knowledge and experiences can be exchanged mutually between SAFIU and foreign FIUs.

5.4.1. Discussion of qualitative results

A number of SAFIU staff provided comments on the effectiveness of international cooperation between SAFIU and foreign FIUs. They believed that SAFIU is exchanging information with non-Egmont Group members exists, but not to the required extent. As a member of the Egmont Group, FIUs indicate the time limits and request for prompt resolutions by marking the request with urgency codes. Global networks, such as ESW, FIU.Net, SWIFT and IMoLIN have been established to facilitate information exchange. SAFIU, being an Egmont Group member, has to adopt the Best Practices and Principles Manual, the Practices Exchange Manual, which provides guidance on the process of sharing information whilst considering privacy and confidentiality aspects (GAO 2006).

The respondents also felt that at times, there are no regular and continuous visits between SAFIU and investigation units in other countries to familiarising themselves with the updated trends and policies. Further, some SAFIU employees stated that additional training programmes should be organised with foreign agencies in order to gain expertise in the field of terrorism financing and money laundering on the global front.

5.5. Q4 – What suggestions can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism finance?

This section supports the fourth objective of this study regarding suggestions to be proposed to SAFIU to emulate policies for combating financial crimes in a better way (six survey question). In addition, this section discusses the type of suggestions proposed to SAFIU to formulate policies that can better combat money laundering and terrorism financing whilst ensuring compliance with the 40+9 FATF Recommendations. The overall opinion of staff members is that 4.73 indicated a strong agreement with this notion.

Interestingly, the feedback from SAFIU staff indicated their strong agreement with the provision of financial and technical resources by the MOI (maximum average of 5.0). This is in support of FATF Recommendation 30 Article 1, which states that FIUs should be provided with technical and financial resources to perform their functions promptly. In 2010, SAFIU was well resourced with an annual budget of SAR100 million, a significant amount higher than AUSTRAC, which during the same year has an annual budget of A$21 million. By contrast, West African FIUs has been severely affected by inadequate financial resources to perform meritoriously (Shehu, 2010).

The feedback also indicated a strong agreement with increased cooperation and coordination between SAFIU and foreign FIUs by the signing of MOUs (an average of 4.95), suggesting that an increase in cooperation between SAFIU and other FIUs. FATF Recommendation 40 Article 1 echoes the importance of FIUs striving towards providing the widest possible support of international cooperation to their foreign counterparts. With the recent membership in Egmont Group, the effectiveness of SAFIUs cooperation has increased significantly with MOUs being signed with partner countries and therefore enabling prompt exchange of information and experience with partner FIUs. Upon gaining membership, SAFIU requested MOUs with 60 foreign FIUs.

The responses of SAFIU staff also reflect a strong agreement that SAFIU will improve its efficiency if direct access to financial information is granted (average of 4.81). This is due to SAFIU not having the authority to access financial information

directly, as it has to request this information from other supervising bodies as per Article 8.1 the of Saudi AML Law. In spite of superseding financial confidentiality and secrecy laws, SAFIU staff strongly felt that gaining direct access to financial information would eliminate delays in receiving information.

Other responses suggest that there is a strong agreement with guidance provided by SAFIU to businesses for monitoring and reporting STRs related to terrorism financing and money laundering (average of 4.59). This is accordance with FATF Recommendation 26 Article 2, which states that FIUs should provide guidance to the private sector regarding specifications and styles of reporting and procedures to be followed. The findings are inconsistent with the 2010 MENAFATF report, which identified private institutions lacking a clear understanding about transaction monitoring and differentiating between STRs. This was especially the case, since only one STR was received from non-bank entities in 2010, and indicates a lack of supporting, governance and training assistance being provided by the supervisory agency MOCI.

With regards to increasing participation of SAFIU staff in local and international seminars and conferences, the feedback indicated that the staff strongly agreed with this notion (average of 4.54). SAFIU staff suggested that an increase of participation in conferences would be a significant step towards combating and formulating policies for terrorism financing and money laundering. Participation in such forums also constitutes compliance to the World Bank who emphasised on the importance of participating in seminars.

Lastly, the responses from SAFIU staff reflect their strong agreement of operating their offices in major cities of KSA to streamline their processes and improve efficiency (average of 4.45). With a single local office currently located in Riyadh, staff proposed that SAFIU should expand its operations into other major cities by following the footsteps of the Prosecution Authority, which currently has offices across 13 provinces. Though this activity requires a large source of funds and expertise, it would enable SAFIU to pay greater attention by raising the level of awareness in AML and CTF risks regionally. It would also be a significant move towards combating terrorism financing, as Saudi Arabia has borders with several

countries and setting up offices across the country could complement SAFIUs efforts. This claim is also supported by the figures cited in the 2010 MENAFATF report regarding the number of cases related to money laundering according to city. Between 2004 and 2008, the second largest city, Jeddah, recorded the highest number of money laundering related cases - 105 cases. This approach is also evident in other FIUs such as AUSTRAC, which has offices operating across five major cities.

5.6. Chapter summary

This chapter discussed the quantitative and qualitative results of the respondents prior to discussing the similarities and differences between what other FIUs practice when complying with International Standards. The findings have generally identified that SAFIU is effective in receiving, analysing, disseminating and cooperating with external agencies in money laundering and terrorism finance activities. SAFIU was also generally deemed compliant with International Standards as set by FATF 40+9 Recommendations. Similarly, the findings were consistent with the MENAFATF Mutual Evaluation Report, which evaluated AML and CTF measures in place within the KSA. The following chapter (Chapter 6: Recommendations and Conclusions) provides a number of recommendations deduced from the study. These are presented in the following chapter.

CHAPTER 6: RECOMMENDATIONS AND CONCLUSION

6.1. Introduction

In light of the results of this study, the researcher suggests a number of recommendations to increase the effectiveness of SAFIU in combating money laundering and terrorism financing. This will be followed by a summary and a conclusion of the study.

6.2. Recommendations

6.2.1. To SAFIU

It is suggested that SAFIU should:

- Provide additional extensive training courses to enhance staff knowledge on money laundering and terrorism financing.
- Increase the number of staff in the Reports Division to ensure prompt and efficient processing of suspicious transactions.
- Promote awareness among financial and commercial institutions on reporting and monitoring suspicious transactions through increased guidelines and best practice publications.
- Participate in international seminars and forums to gain insights on emerging trends, effective AML and CTF policies, and develop collaborative MOUs.
- Regularly and consistently publish reports that comprehensively detail information relating to latest trends, models, case studies, and statistics and training courses.
- Initiate appropriate protocols for conducting further analysis and investigations that expand on money laundering and terrorism finance typologies.
- Actively engage and participate in experience exchange with foreign FIUs by conducting more frequent visits and exchange programs.
- Introduce electronic mechanism of receiving STRs from reporting bodies to enhance analysis and investigation.
- Conduct outreach programs for the public and provide more information on SAFIUs roles, objectives, activities and regulatory requirements.

6.2.2. To PCCML and supervising authorities

It is suggested that the PCCML and Supervisory Authorities:

- PCCML to play an active role in supporting SAFIUs activities, specifically in relation to awareness, training and non-compliance of the AML and CTF framework.
- PCCML to negotiate additional programmes and agreements on exchanging experience between SAFIU and foreign FIUs.
- PCCML and supervisory bodies to regularly update financial and non-financial institutions on the latest money laundering and terrorism finance information.
- PCCML to ensure that supervisory authorities implement strategies that address any compliance shortcomings.
- Supervisory authorities to investigate monitor and govern the AML and CTF compliance of financial and non-financial institutions.
- Supervisory authorities to raise awareness and knowledge on AML and CTF reporting requirements through continuous training, seminars and workshops.

6.2.3. To the Kingdom of Saudi Arabia

It is suggested that the KSA:

- Grant SAFIU direct access to government databases and financial information thereby increasing the effectiveness and autonomy of SAFIU.
- Authorise the development and implementation of interlinked databases that extend across various national security agencies.
- Open FIU branches in other major cities within the Kingdom.

6.2.4. To future researchers

It is suggested that the future researchers:

- Examine the compliance of financial institutions to the International Standards (FATF 40+9 Recommendations) through SAMA.
- Examine the compliance of non-financial institutions (Businesses) to the International Standards (FATF 40+9 Recommendations) through MOCI.

6.3. Final summary and conclusion

In chapter one, the thesis commenced by providing an introduction of the aim and purpose of the study. The aim of the thesis was to investigate and examine the effectiveness of SAFIU, the principal agency in the KSA that deals with the

prevention of money laundering and terrorism financing. By focusing on the effectiveness of SAFIU, this thesis evaluated the compliance of the KSA's legal framework to the International Standards of the 40+9 FATF Recommendations.

Chapter two (literature review) reviewed and the discussed existing literature in order to define, illustrate and provide context on the functions of FIUs. The chapter also discussed the background and implications of money laundering and terrorism finance prior to providing evidence of the practices of FIUs in receiving, analysing and disseminating STRs. Chapter three (methodology) detailed the procedure and methodology used for the study by describing the research design and instruments utilised, as well as the validity, translation and process of data collection. Chater four (findings) reported on the data analysis acquired and then discussed the quantitative and qualitative results of the survey respondents, linking the results to the literature review conducted earlier. This approach enabled the researcher to develop recommendations for various parties within the KSA.

The study yielded a set of results based on the functional and personal characteristics of staff members in evaluating the effectiveness of SAFIU. The results in general indicated a strong agreement of compliance to International standards in the core areas of receiving, analysing and disseminating in combating money laundering and terrorism finance activities. It was also found that SAFIU was effective in confiscating and freezing accounts and cooperating with other government agencies. Despite SAFIU undertaking activities consistent with the majority of the Recommendations, respondents highlighted a number of shortcomings. SAFIU needs to ensure that annual reports and guidance manuals detailing current trends, cases and topologies are regularly and consistently published. SAFIU, with its PCCML membership, needs to ensure awareness and compliance of supervising authorities to ensure that reporting entities are monitored and governed to comply with the International Standards. Staff performance and AML and CTF awareness could also be improved with better exchange programmes with foreign FIUs, and greater attendance at international seminars and forums. SAFIUs effectiveness in cooperating with other FIUs in foreign countries was also evaluated. It was observed that SAFIU demonstrated its ability and willingness to cooperate and liaise with foreign FIUs through the Egmont Group.

In conclusion, the results of this study indicate that SAFIU is largely compliant to the International Standards of the 40+9 FATF Recommendations.

REFERENCES

Abadie, A and Gardeazabal, J 2008, 'Terrorism and the world economy', *European Economic Review,* Vol. 52, No. 1, pp. 1-27.

Ai, L., Broome, J and Yan, H 2010, 'Carrying out a risk-based approach to AML in China: partial or full implementation?' *Journal of Money Laundering Control*, Vol. 13, No. 4, pp. 394-404.

Ajayi, K and Abdulkareem, H 2010, 'Insulating the vaults from the tide of dirty money: are the floodgates secure?' *Journal of Money Laundering Control*, Vol. 13, No. 1, pp. 33-44.

Alowain, A 2005, 'An Examination of Money Laundering Activities: The United Nation's Perspective and Saudi Arabia', *A Masters Project Report Presented to the Department of Criminal Justice,* Carlifonia State University.

Ashford, Mary-Wynne and Dauncey, Guy 2006, *Enough Blood Shed: 101 Solutions to Violence, Terror and War*, New Society Publishers, Canada.

AUSTRAC 2005, *Annual Report 2004-05*, Viewed 11 May 2011 http://www.austrac.gov.au/files/austrac_annual_report_2005.pdf

Beall, J 2007, *Cities, Terrorism and Urban Wars of the 21st Century*, Working Paper No. 9, Series 2, Crisis States Research Centre, LSE: London.

Beare, M and Schneider, S 2007, *Money Laundering in Canada: Chasing Dirty and Dangerous Dollars*, Canada: University of Toronto Press Inc.

Biagioli, A 2006, 'Methodological innovation and effective action', *Journal of Financial Crime,* Vol. 13, No. 3, pp. 369-374.

Bolodeoku, O 2009, '*The war against corruption in Nigeria: a new role for the FIRS?', Journal of Money Laundering Control* , Vol. 2, No. 4, pp. 417-431.

Bowers, C 2009, 'Hawala, Money Laundering, And Terrorism Finance: Micro-Lending As An End To Illicit Remittance', Vol. 37, No. 3, pp. 379-419.

Broom, J 2005, *Anti-money Laundering: International Practice and Policies*, Thomson, Hongkong.

Bunt, H 2008, 'A Case Study on the misuse of hawala banking' *International Journal of Social Economics'* Vol. 35, No. 9, pp. 691-702.

Chaikin, D 2009, 'How effective are suspicious transaction reporting systems?' *Journal of Money Laundering Control,* Vol. 12, No. 3, pp. 238-253.

Chatain P., Mcdowell J., Mousset C., Schott P. A and De Willbois, E. V 2009, *Preventing Money Laundering and terrorist Financing*, The World Bank, Washington.

Chlabicz, J and Filipkowski, W 2001, **'**The Polish Financial Intelligence Unit: A New Institution in the Polish Legal System', *Journal of Money Laundering Control*, Vol. 5, No. 2, pp. 150-157.

Cronbach, L.J 1951, 'Coefficient alpha and the internal structure of tests', *Psychomterika*, Vol. 16, Issue. 3, pp. 297-334.

Cohen, L., Manion, L., and Morrison, K 2007, *Research Methods in Education*, Routledge, New York.

Commonwealth Secretariat 2006, *Combating Money Laundering and Terrorist Financing: A Model of Best Practices for the Financial Sector, the Professions and other Designated Businesses*, 2nd edition, Commonwealth Secretariat, Pall Mall, London.

Cordesman, A. H 2003a, *Saudi Arabia and the challenge of terrorism: Reacting to the "9/11 report"*, viewed 21 June 2011, http://csis.org/publication/saudi-arabia-and-challenge-terrorism-reacting-911-report

Cordesman, A. H 2003b, *Saudi Arabia Enters the Twenty-first Century: The Political, Foreign Policy, Economic and Energy Dimensions*, Greenwood Publishing Group, USA.

Cordesman, A. H 2009, *Saudi Arabia: National Security in a Troubled Region*, Center for Strategic and International Studies, Washington DC.

Cordesman, A. H and Obaid, N. E 2005, *National Security in Saudi Arabia: Threats, Responses, and Challenges*, Greenwood Publishing Group, New York.

Demetis, D and Angell, I 2006, 'AML-related technologies: a systemic risk,' *Journal of Money Laundering Control*, Vol. 9, No. 2, pp. 157-172.

Diekman, P 1999, 'Corruption and Money Laundering: The Role of the Private Sector', *Journal of Money Laundering Control*, Vol. 3, No. 2, pp. 115-124.

Diekman, P 2008, *Protecting financial market integrity: Roles and responsibilities of auditors*, Kluwer, UK.

Drakos, K 2004, 'Terrorism-induced structural shifts in financial risk: airline stocks in the aftermath of the September 11th terror attacks', *European Journal of Political Economy*, Vol. 20, No. 2, pp. 435–446.

Duthel, H 2008, *The Profesionals Politic & Crime International Money Laundering*, Lulu.com.

Egmont Group, n.d, *FIUs in Action*, viewed 15 March 2011, http://www.egmontgroup.org

FATF 2000, '*Report on Money Laundering Typologies 1999-2000',* viewed 2 February 2011, http://www.oecd.org/dataoecd/29/37/34038120.pdf

Favarel-Garrigues G., Godefroy T, and Lascoumes, P 2008, 'Sentinels in the banking industry. Private actors and the fight against money laundering in France', *British Journal of Criminology*, Vol. 48, pp. 1-19.

Field, A 2009, *Discovering Statistics Using SPSS*, Sage Publications, London, UK.

FINTRAC 2001, *Annual Report 2001*, FINTRAC, Ottawa.

FINTRAC 2003, *Annual Report 2003*, FINTRAC, Ottawa.

FIU Germany 2004, *2004 Annual Report: FIU Germany*, Viewed 8 May 2011, http://www.bka.de/nn_195296/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/FIU/fiuAnnualReport2004,templateId=raw,property=publicationFile.pdf/fiuAnnualReport2004.pdf>

Fiu.net, *History*, viewed 20 April 2011, http://www.fiu.net/welcome/history

Forman, M 2006, 'Combating terrorist financing and other financial crimes through private sector partnerships', *Journal of Money Laundering Control*, Vol. 9, No.1, pp. 112-118.

Frey, B, Luechinger, S and Stutzer, A 2007,'Calculating Tragedy: Assessing the costs of Terrorism', *Journal of Economic Surveys*, Vol. 21, No. 1, pp. 1-24.

GAO 2006, 'International Financial Crime', *GAO*. http://www.gao.gov/new.items/d06483.pdf

Gelemerova, Liliya 2008, On the frontline against money-laundering: the regulatory minefield, *Crime Law and Social Change*, Vol. 52, No. 1, pp. 33-55.

Gerwien, R 2008, *A Painless Guide to Statistics*, viewed 5 January 2011, http://www.bates.edu/~ganderso/biology/resources/statistics.html

Gottselig, G and Underwood, S 2004, *Financial Intelligence Untis: An Overview*, International Monetary Fund, Washington DC.

Gotz, E and Jonsson, M 2009, 'Political factors affecting AML/CTF efforts in post-comunist Eurasia', *Journal of Money Laundering Control*, Vol. 12, No.1, pp. 59-73.

Griffith, I. L 1997, *Drugs and Security in Caribbean: Sovereignty under siege*, The Pennsylvania State University Press, Pennsylvania.

Gubbay, A 2007, 'Zimbabwe: Report on Money Laundering (No. 61)', *Journal of Money Laundering Control,* Vol. 1, No. 3, pp. 277-286.

Gurule, J 2008, *Unfunding Terror: The legal response to the financing of global terrorism*, Edward Elgar publishing, Cheltenham, UK.

He, P 2005, 'The Suspicious Transactions Reporting System, *Journal of Money Laundering Control,* Vol. 8, No. 3, pp. 252-259.

He, P 2010, 'A typological study on money laundering', *Journal of Money Laundering Control,* Vol. 13, No. 1, pp. 15-32.

Henry, G.T 1990, *Practical Sampling*, Newbury Park, CA.

Herman, D 2002, *Taxing Portfolio Income in Global Financial Markets*, IBFD Publications, Amsterdam.

Hopton, Duog 2009, *Money Laundering: A Concise Guide for All Business*, Gower Publishing, UK.

IMF 2003, *Suppressing the Financing of Terrorism: A Handbook for Legislative Drafting*, International Monetary Fund.

IMF 2004, *Financial Intelligence Untis: An Overview*, International Monetary Fund, Washington DC.

IMF 2008, *United Arab Emirates: Detailed assessment report on Anti-Money Laundering and Combating the Financing of Terrorism*, International Monetary Fund Country Report No. 08/305, Washington DC.

IMF 2011, *The IMF and the Fight Against Money Laundering and the Financing of Terrorism,* viewed 25 March 2011, http://www.imf.org/external/np/exr/facts/aml.htm

Inter-American Development Bank 2004, *Economic and Social Progress in Latin America*, IDB, Washington DC.

Interpol 2010, *Anti-Money Laundering Unit*. (n.d.), viewed 10 April 2011, http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/Unit.asp

Interpol 2011, *Alternative remittance systems distinguishing sub-systems of ethnic money laundering in Interpol member countries on the Asian continent,* viewed 2 January 2011, http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp

Interpol 2011, *Data exchange*, viewed 5 August 2011, http://www.interpol.int/layout/set/print/INTERPOL-expertise/Data-exchange/I-24-7

Jamieson, S 2004, 'Likert scales: how to (ab)use them', *Medical Education*, Vol. 38, No. 12, pp. 1217–1218.

Jensen, N 2006, *The Egmont Group International Bulletin,* viewed April 18, 2011, from The Egmont Group International Bulletin: http://www.egmontgroup.org/library/download/20

Jensen, N and Png, Cheong-Ann 2011, 'Implementation of the FATF 40+9 Recommendations', *Journal of Money Laundering Control*, Vol. 14, No. 2, pp. 110-120.

Johnson, B and Christensen, L 2007, *Educational Research: Quantitative, qualitative, and mixed approaches*, 3rd edition, SAGE Publications, London.

Johnson, J 2008, 'Is the global financial system AML/CFT prepared?', *Journal of Financial Crime,* Vol. 15, No. 1, pp. 7-21.

Jost, P. M and Sandhu, H. S 2000, '*The hawala alternative remittance system and its role in money laundering'* viewed 10 June 2011, http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp

Kalin, C., Muller, W and Goldsworth, J 2007, *Anti-money laundering: International law and practice*, John Wiley & Sons, West Sussex.

Kennedy, A 2007, 'Winning the information wars Collecting, sharing and analysing information in asset recovery investigations', *Journal of Financial Crime*, Vol. 14, No. 4, pp. 372-404.

Kishima, K 2004, 'Japan's Efforts in the Global Fight against Money Laundering and Terrorist Financing', *Journal of Money Laundering Conrol*, Vol. 7, No. 3, pp. 261-263.

Koh, J 2006, *Suppressing terrorist financing and money laundering*, Springer Berlin Heidelberg, Germany.

Leong, A 2007, 'Chasing dirty money: domestic and international measures against money laundering', *Journal of Money Laundering Control*, Vol. 10, No. 2, pp. 140-156.

Mann, H. B and Whitney, D. R 1947, 'On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other', *The Annals of Mathematical Statistics*, Vol. 18, pp. 50–60.

Magnusson, D 2009, 'The costs of implementing the anti-money laundering regulations in Sweden', *Journal of Money Laundering Control*, Vol. 12, No. 2, pp. 101-112.

Masciandaro, D 2005, 'Financial Supervisory Unification and Financial Intelligence Units', *Journal of Money Laundering Control*, Vol. 8, No. 4, pp. 354-370.

Masciandaro, Donato, Takats, Elod and Unger, Brigitte 2007, *Black Finance: The Economics of Money Laundering*, Edward Elgar Publications, UK.

McCann, Hilton 2006, *Offshore Finance*, Cambridge University Press, USA.

MENAFATF 2010, 'Anti-Money Laundering and Combating the Financing of Terrorism: Kingdom of Saudi Arabia', *Mutual Evaluation Report*, MENAFATF.

MENAFATF 2011, MENAFATF Newsletter, Issue. 3, viewed 1 June 2011, http://www.menafatf.org/images/UploadFiles/MENAFATF_Newsletter_Issue3_English.pdf

Merlonghi, G 2010, 'Fighting financial crime in the age of electronic money: Opportunities and limitations', *Journal of Money Laundering Control*, Vol. 13, No. 3, pp. 202-214.

Mitsilegas, V 1999, 'New forms of transnational policing: The emergence of Financial Intelligence units in European union and the challenges for human rights :part 1', *Journal of Money Laundering Control*, Vol. 3, No. 2, pp.147-160.

Mitsilegas, V 2003, Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles, Kluwer Law International, New York.

MOFA 2005, '*Counter-terrorism international conference',* viewed 25 June 2011, http://www.mofa.gov.sa/sites/mofaen/aboutkingdom/kingdomforeignpolicy/antiterrorism/Pages/AntiTerrorismConference35026.aspx

MOI 2003, *The Law of Combating Money Laundering*, MOI.

MOI 2007, *The Annual report of Saudi Arabian Financial Intelligence*, viewed 12 January 2011, http://www.moi.gov.sa/wps/wcm/connect/81d5ed004dcfb7d188e99e2b6135edb7/%D8%A7%D9%84%D8%AA%D9%82%D8%B1%D9%8A%D8%B1+2007.pdf?MOD=AJPERES&CACHEID=81d5ed004dcfb7d188e99e2b6135edb7.

Muller, W., Kalin, C., and Goldsworth, J 2007, Anti-money laundering: international law and practice, John Wiley & Sons, UK.

Murphy, D 2006, 'Disclosure and sharing of sensitive information Revisiting risk in co-operating Regulatory regimes', *Journal of Financial Crime*, Vol. 13, No. 4, pp. 420-441.

Nigerian Financial Intelligence Unit (NFIU) Newsletter 2008, 'NFIU-News', *Nigerian Financial Intelligence Unit Newsletter*, Issue 2, Vol.3.

Odeh, I 2010, *Anti-Money Laundering and Combating Terrorist Financing For Financial Institutions*, Dorrance Publishing Co., Pittsburgh, Pensylvania.

Parandeh, C 2009, 'Hawala: The fund transfer methodology that evades surveillance', *Journal of Corporate Treasury Management*, Vol. 3, No. 1, pp. 22-32.

Parkman, T and Peeling, G 2007, *Countering Terrorist Financing: a training handbook for financial services*, Gower Publishing, Aldershot, Hampshire.

Perry, F 2005, *Research in Applied Linguistics: Becoming a Discerning Consumer*, Lawrence Eribaum Associates, USA.

Pieth, M., Thelesklaf, D and Ivory, R 2009, *Countering Terrorist Financing: The Practitioner's Point of View,* Germany: Peter Lang AG.

Prados, A, B and Blanchard, C, M 2004, *Saudi Arabia: Terrorist Financing Issues, viewed 3 Jan 2011*, http://www.fas.org/irp/crs/RL32499.pdf

Preller, S 2008, 'Comparing AML legislation of the UK, Switzerland and Germany', *Journal of Money Laundering Control*, Vol. 11, No. 3, pp. 234-250.

Qorchi, M. E, Maimbo, S. M and Wilson, J. F 2003, *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, IMF Multimedia services Washington, DC.

Razavy, M 2005, 'Hawala: An underground haven for terrorists or social phenomenon?', *Crime, law & Social Change*, Vol. 44, No. 3, pp. 277-299.

Reuter, T and Truman, T 2004, *Chasing dirty money: the fight against money laundering*, Institute for International Economics, Washington.

Ross, S and Hannan, M 2007, 'Money laundering regulation and risk-based decision-making', *Journal of Money Laundering Control*, Vol. 10, No. 1, pp. 106–115.

Ryder, Nicholas 2011, *Financial Crime in the 21st Century: Law and Policy*, Edward Elgar Publishing, UK.

SAMA 2004, *A report on initiatives and actions taken by Saudi Arabia to combat terrorist financing and money laundering*, SAMA, viewed 4 February 2011, http://www.saudiembassy.net/files/PDF/SAMA_INITIATIVES_BY_KSA_UP_DATED_APRIL_2004.pdf

Sapkota, Dharma 2010, *Nepal FIU news letter*, Viewed 2 April 2011 http://www.nrb.org.np/fiu/pdffiles/news_letter_May_2010.pdf

Sathye, M and Patel, C 2007, 'Developing financial intelligence: an assessment of the FIUs in Australia and India', *Journal of Money Laundering Control,* Vol. 10, No. 4, pp. 391-405.

Scherrer, Amandine 2009, *G8 against Transnational Organised Crime*, Ashgate Publishing, UK.

Schneider, F 2009, 'Turnover of organised crime and money laundering: some preliminary empirical findings', *Public Choice*, Vol. 144, No. 3, pp. 1-21.

Schott, Paul 2006, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, World Bank.

Sham, A 2006, 'Money laundering laws and regulations: China and Hong Kong', *Journal of Money Laundering Control,* Vol. 9, No. 4, pp. 379-400.

Shanmugham, B 2004 'Hawala and Money Laundering: A Malaysian Perspective', *Journal of Money Laundering Control*, Vol. 8, No. 1, pp. 37-47.

Shanumgam, B and Thanasegaran, H 2008, 'Combating money laundering in Malaysia', *Journal of Money Laundering Control,* Vol. 11, No. 4, pp. 331-344.

Sharman, J and Chaikin, D 2009, 'Corruption and Anti-Money-Laundering Systems: Putting a Luxury Good to Work', *An International Journal of Policy, Administration, and Institutions*, Vol. 22, No. 1, pp. 27-45.

Shehu, A 2010, 'Promoting financial sector stability through an effective AML/CFT regime', *Journal of Money Laundering Control,* Vol. 13, No. 2, pp. 139-154.

Siegel, Larry J 2008, *Criminology,* Belmont, CA.

Simser, J 2006, 'The significance of money laundering: The example of Philippines', *Journal of Money Laundering Control,* Vol. 9, No. 3, pp. 293-302.

Smith, P 2007, 'Terrorism Finance: Global Responses to the Terrorism Money Trail', in James J. Forest (ed.), *Countering terrorism and insurgency in the 21st century: Combating the sources and facilitators,* USA: Greenwood Publishing Group, Inc.

SOCA 2011, SOCA: Serious Organised Crime Agency, viewed 3 Sep 2011, http://www.soca.gov.uk/about-soca/the-uk-financial-intelligence-unit/frequently-asked-questions-faqs

Sorel, J. M 2003, 'Some Questions About the Definition of Terrorism and the Fight against its Financing', *European Journal of International Law*, Vol. 14, No. 2, pp. 365-378.

Sproat, P 2007, 'The new policing of assets and the new assets of policing: A tentative financial cost-benefit analysis of the UK's anti-money laundering and asset recovery regime', *Journal of Money Laundering Control,* Vol. 10, No. 3, pp. 277-299.

Sproat, P 2010, 'Counter-terrorist finance in the UK A quantitative and qualitative commentary based on open-source materials', *Journal of Money Laundering Control,* Vol. 13, No. 4, pp. 315-335.

Stefanou, C 2010, 'Section ii. Focus on enforcement Databases as a means of combating organised crime within the EU', *Journal of Financial Crime,* Vol. 17, No.1, pp. 100-115.

Subbotina, N 2008, 'Development of anti-money laundering regime in Russia', *Journal of Money Laundering Control,* Vol. 11, No. 4, pp. 358-370.

Tang, J and Ai, L 2010, 'Combating money laundering in transition countries: the inherent limitations and practical issues', *Journal of Money Laundering Control,* Vol. 13, No. 4, pp. 394-404.

Thanasegaran, H and Shanmugam, B 2008, 'Exploitation of the insurance industry of money laundering: the Malaysian perspective', *Journal of Money Laundering Control,* Vol. 11, No. 2, pp. 135-145.

The Joint Forum 2003, 'Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism', *Basel Committee on Banking Supervision*, pp. 1-10.

Thony, J 1996, Processing Financial Information in Money Laundering Matters: The Financial Intelligence Unit', *European Journal of Crime, Criminal Law and Criminal Justice,* Vol. 4, No. 3, pp. 257-282.

Tittle, C and Hill, R 1967, 'Attitude Measurement and Prediction of Behaviour: An Evaluation of Conditions and Measurement Techniques', *Sociometry,* Vol. 30, No. 2, pp. 199-213.

Trehan, J 2002,'Underground and parallel Banking Systems', *Journal of Money Laundering Control,* Vol. 10, No. 1, pp. 76-84.

UN 1999, *International Convention for the Suppression of the Financing of Terrorism*, viewed 3 March 2011, http://www.un.org/law/cod/finterr.htm

UNODC 2007, *An Overview of the UN Conventions and other International Standards concerning Anti-Money Laundering and Countering the Financing of Terrorism*, UNODC, viewed 3 March 2011, http://www.imolin.org/pdf/imolin/Overview%20Update_0107.pdf

Vaccani, M 2009, *Alternative Remittance Systems and Terrorism Financing*, The World Bank Working Paper no. 180, Washington DC.

Verdugo-Yepes, C 2008, 'Enhancing international cooperation in the fight against the financing of terrorism', *Journal of Global Change and Governance*, Vol. 1, No. 3, pp. 1-23.

Verhage, A 2009a, 'Compliance and AML in Belgium: a booming sector with growing pains', *Journal of Money Laundering Control*, Vol. 12, No. 2, pp. 113-133.

Verhage, A 2009b, 'Supply and Demand- anti - money laundering by the compliance industry', *Journal of Money Laundering Control*, Vol. 12, No. 4, pp. 371-391.

Viles, T 2008, 'Hawala, hysteria and hegemony', *Journal of Money Laundering Control*, Vol. 11, No. 1, pp. 25-33.

Wellington, J 2000, *Educational Research: Contemporary Issues and Practical Approaches*, Continuum, London.

Wesley, J. Anderson 2010, *Disrupting Threat Finances: Utilization of Financial Information to Disrupt Terrorist Organizations in the Twenty-First Century*, Fort Leavenworth, Kansas.

Wilson, C and Rattray, K 2007, 'The Caribbean Financial Action Task Force: its mission, operations and future prospects', *Journal of Financial Crime*, Vol. 14 No. 3, pp. 227-249.

World Bank 2004, *Building an effective anti-money laundering and counter-terrorism financing regime in afghanistan*, viewed 10 April 2011, http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/afghan_aml.pdf

World Bank 2009, *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide*, World Bank Publications, Washington DC.

Yan, L., Ai, L and Tang, J 2011, 'Risk-based AML regulation on internet payment services in China', *Journal of Money Laundering Control*, Vol. 14, No. 1, pp. 93-101.

Zagaris, Bruce 2010, *International White Collar Crime: Cases and Materials*, Cambridge, New York.

LIST OF APPENDICIES

Kingdom of Saudi Arabia
Ministry of Interior

Anti-Money Laundering Law & its Implementing Regulations

Royal Decree No. M/39
25 Jumada II *1424 / 23 August 2003*

Article (1):
The following terms and phrases, wherever mentioned in this Law, shall have the meanings expressed next to them, unless the context requires otherwise:

1. **Money Laundering:**
   Committing or attempting to commit any act for the purpose of concealing or disguising the true origin of funds acquired by means contrary to *Shari'ah* or law, thus making them appear as if they come from a legitimate source.

2. **Funds:**
   Assets or properties of whatever type, tangible or intangible, movable or immovable, as well as legal documents and deeds proving ownership of the assets or any right pertaining thereto.

3. **Proceeds:**
   Any funds obtained or acquired directly or indirectly by committing a crime punishable pursuant to the provisions of this Law.

4. **Means:**
   Anything used or prepared for use in any form for committing a crime punishable pursuant to the provisions of this Law.

5. **Financial and Non-Financial Institutions:**
   Any institution in the Kingdom undertaking one or more of the financial, commercial or economic activities, such as banks, money exchange, investment and insurance companies, commercial companies, sole proprietorships, vocational activities or any other similar activity specified by the Implementing Regulations of this Law.

6. **Transaction:**
   Any disposal of funds, possessions or proceeds in cash or in-kind, including, for example: deposit, withdrawal, transfer, sale, purchase, lending, exchange or use of safe deposit boxes and the like, as specified by the Implementing Regulations of this Law.

7. **Criminal Activity:**
   Any activity constituting a crime punishable by *Shari'ah* or law, including the financing of terrorism, terrorist acts and terrorist organizations.

8. **Preventive Seizure:**
   Temporary ban on transport, transfer, exchange, disposal, movement, possession or temporary seizure of funds and proceeds, pursuant to an order issued by a court or a competent authority.

9. **Confiscation:**
   Permanent dispossession and deprivation of funds, proceeds or means used in a crime, pursuant to a judicial judgment rendered by a competent court.

10. **Monitoring Agency:**
    The governmental agency empowered to license, monitor or supervise financial and non-financial institutions.

11. **Competent Authority:**
    Any governmental agency entrusted, according to its jurisdiction, with combating money laundering transactions.

1-1 one of the funds in paragraph (2) of this article financial instruments negotiable bearer or endorsed without restriction in favor of an unknown or beneficiary becomes the right of ownership when extradition is not documentation contained the names of the beneficiaries such as traveler's checks, checks, Sear, and payment orders.

1-2 The following are deemed activities provided for in paragraph (5) of this Article:

(a) Acceptance of deposits, borrowing, opening of accounts.
(b) Insurance, finance lease.
(c) Money transfer services.
(d) Issuance and management of means of payment (credit cards, traveler's checks, bank cards).
(e) Issuance of guarantees and credits.
(f) Trading or dealing in monetary instruments or dealing in foreign currencies.
(g) Trading and financial brokerage.
(h) Real estate transactions and Trust service.
(i) Dealing in valuable metals, precious stones or rare commodities, like antiques.

(j). Trade in goods with high value such as luxury cars and goods offer in auction houses.
(k) Law practice and company service.
(l) Accounting and auditing.

1-3 The following are deemed activities provided for in paragraph (6) of this Article:

(a) Mortgage.
(b) Transfer between accounts.
(c) Gifts.
(d) Currency exchange.
(e) Trading securities.
(f) Purchase or sale of any stocks, securities or certificates of deposits.
(g) Authentication of contracts and power of attorney by the notary publics.

1-4 The authority in charge of preventive seizure provided for in paragraph (8) of Article (1), is the Bureau of Investigation and Public Prosecution, pursuant to what is provided for in Article 12 of The Anti-Money Laundering Law and its Implementing Regulations.

Article (2):

Anyone who commits any of the following acts shall be committing a money laundering crime:

(a) Conducting any transaction involving funds or proceeds, with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(b) Transporting, acquiring, using, keeping, receiving, or transferring funds or proceeds with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(c) Concealing or disguising the nature of funds, proceeds or their source, movement, ownership, place or means of disposal, with the knowledge that they are the result of a criminal activity or from unlawful or illegal sources.
(d) Financing terrorism, terrorist acts and terrorist organizations.
(e) Participating by way of agreement, aiding and abetting, incitement, counsel, advice, facilitating, collusion, covering or attempting to commit any of the acts stated in this Article.

2-1 Financing terrorism, terrorist acts and terrorist organizations includes funds resulting from lawful sources.

2-2 Knowledge can be inferred from the objective and factual conditions and circumstances; thus creating an element of criminal intent constituting one of the crimes provided for in this Article.

2-3 Examples of the criminal activities or the unlawful or illegal sources whereby the dealing in funds resulting therefrom is deemed a money laundering crime are as follows:

(a) Crimes provided for in Article (1) of the Implementing Regulations of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, for the year 1988, which was ratified by the Council of Ministers' Resolution No (168) dated 11/8/1419H.
(b) Organized crimes provided for in the United Nations Convention for Controlling Transnational Organized Crimes (Palermo Convention) issued in December 2000 and ratified by Royal Decree No. (m / 20) and the date of e 24/3/1425.
(c) The crimes set out in paragraph (5) of Article II of the International Convention on the Suppression of the Financing of Terrorism, ratified by Royal Decree No. (m / 62) and the date of e 18/7/1428.
(d) Smuggling, manufacturing, trading in or promoting intoxicants.
(e) Crimes of money counterfeiting provided for in the Royal Decree No (12) dated 12/7/1379H.
(f) Forgery crimes provided for in the Anti-Forgery Law issued by Royal Decree No (114) dated 26/11/1380H amended by Royal Decree No (53) dated 5/11/1382H.
(g) Bribery crimes provided for in the Anti-Bribery Law issued by Royal Decree No (36) dated 29/12/1412H.
(h) Smuggling weapons and ammunitions or explosives, or manufacturing or trading in them.
(i) Procurement and preparation of brothels or exercising of debauchery.
(j) Plundering or armed robbery.
(k) Thefts.
(l) Defraud and swindling.

(m) Embezzlement of public funds of government bodies or that which the state contributes to, as well as private funds of companies and commercial establishments and the like.

(n) Engaging in banking activities illegally, as provided for in Article (2) of the Banks Monitoring Law, issued by Royal Decree No (5) dated 22/2/1386H

(o) Mediation in the securities without a license provided for in Article (31) and dealing in security based on information obtained from an insider provided for in Article (50) of the Capital market law by Royal Decree No. (M / 30) and the date of e 2/6/1424.

(p) Mediation in the insurance business without a license provided for in Article (18) of the Cooperative Insurance Companies law by Royal Decree No. (m / 32) and the date of 2/6/1424 e.

(q) Crimes related to commercial activities such as fraud in brands, weights and prices as well as imitation of goods and commercial concealment as provided for in Article (1) of Anti-Commercial Concealment Law, issued by Royal Decree No (M/49) dated 16/10/1409H .

(r) Smuggling provided for in the Unified Customs Law for the GCC States, issued by Royal Decree No (241) dated 26/10/1423H
Tax evasion crimes.

Article (3):

Anyone who commits or participates in any of the acts specified in Article (2) of this Law, shall be committing a money laundering crime, including chairmen of the boards of directors of financial and non-financial institutions, board members, owners, employees, authorized representatives, auditors or their hired hands who act in these capacities, without prejudice to the criminal liability of the financial and non-financial institutions for that crime if it has been committed in their names or on their behalf.

3-1 Provisions of this Law and its Implementing Regulations shall apply to financial and non-financial institutions established in the free zones within the Kingdom.

3-2 Provisions of this Law and its Implementing Regulations shall apply to financial and non-financial institutions **and their branches and subsidiaries** operating **within** and outside the Kingdom.

3-3 The crime was committed in the name or on behalf of the financial and non-financial institution for the purpose of direct or indirect material or immaterial gain.

Article (4):

Financial and non-financial institutions shall not conduct any financial or commercial transaction, or otherwise under a false or unknown name. The identity of the clients shall be verified against official documents, at the outset of dealing with these clients or when concluding commercial deals whether directly or on their behalf. Such institutions shall verify the official documents of the corporate entities showing the name of the institution, its address, names of proprietors and managers authorized to sign on its behalf and the like, as provided for in the Implementing Regulations of this Law.

4-1 Financial and non-financial institutions **and professions** shall fully comply with instructions issued by the monitoring entities such as the Saudi Arabian Monetary Agency, Capital Market Authority, Ministry of Commerce and Industry and Ministry of Justice, pertaining to the principle of "know your client" **and due diligence** provided that it shall include the following as a minimum:

4-1-1 Verifying the identities of **all permanent or occasional** clients of financial and non-financial institutions against Valid officially certified original documents proving their identities as follows:

(a) Saudi nationals:

- National identification card or family record.
- Address of the person, place of residence and place of work.

(b) Individual expatriates:

- residence permit (*Iqamah*) or a five-year special residence permit or a passport or National identification for GCC nationals or a diplomatic identification card for diplomats.
- Address of the person, place of residence and place of work.

(c) Corporate persons:

- Licensed companies, establishments and stores:
  - Commercial register issued by the Ministry of Commerce and Industry.
  - License issued by the Ministry of Municipal and Rural Affairs for service establishments and private stores.
  - Articles of association, if any.
  - National identification card for the Saudi national who owns the commercial firm or the licensed service company to ensure that the merchant's name in the commercial register or the licenses is identical to his name and other details in the national identification card and that such card is valid.
  - A list of the persons who own the firm whose names are provided in the articles of association and their amendments, if any, and a copy of the identification cards of each of them.
  - A list of the persons authorized by the owner who are qualified to deal with the accounts, pursuant to what is provided for in the commercial register or according to a power of attorney issued by a notary public, or an authorization made at the bank and a copy of the identification card of each.

- Resident companies:
  - A copy of the commercial register issued by the Ministry of Commerce and Industry.
  - A copy of the articles of association and their annexes.
  - A license activity.
  - A copy of the identification card of the manager in charge.
  - A power of attorney issued by a notary public or a special authorization from the person(s), who, pursuant to the articles of association, have the power to authorize individuals to sign on their behalf.
  - A copy of the identification cards of the firm owners whose names are provided in the articles of association and their amendments.

4-2 Verifying the identity and legal status of actual clients and beneficiaries for all customers defined as the natural person ultimately owning or

controlling a customer or on whose behalf a transaction is being conducted, before opening an account or the initiation of transaction with any financial and non-financial institution.

4-3 Data related to the verification of identity shall be updated periodically or whenever there is a doubts about the accuracy or adequacy of the data obtained in advance at at any stage of dealing with the actual client or true beneficiary, and whenever there is a suspicion of money laundering or terrorist financing regardless Amounts of the limits of the process.

4-4 determine whether any customer is acting on behalf of another person and to take measures to identify and verify the identity of that person, with particular attention to accounts and business relationships operated under power of attorney.

4-5 enhanced due diligence performed for higher-risk categories of customer, business relationships, or transactions.

4-6 Simplified due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

4-7 It shall not be acceptable from an agent, such as a lawyer, an accountant or a broker, and the like, to use the non-disclosure of clients' confidential information as an excuse when completing identity verification data in the manner mentioned above.

Article (5):

Financial and non-financial institutions shall keep, for a period of not less than ten years from the date of completion of the transaction or closing of the account, all records and documents to show the financial dealings, commercial and cash transactions, whether domestic or foreign and, to retain account files, business correspondence and copies of personal identification documents.

5-1 Financial and non-financial institutions shall retain a copy of the personal identification documents of their clients and of any document pertaining to the transactions conducted.

5-2 Financial and non-financial institutions shall maintain a record including all details of the transactions made to ensure:

(a) Fulfillment of the requirements of the Anti-Money Laundering Law.
(b) **Sufficient to** enable **the Financial Intelligence Unit and the investigation and** a judicial authority **to** trace and **reconstruction of** each **transaction.**
(c) Answering, within the specified period, all inquiries made by the Financial **Intelligence** Unit **and the investigation** or a judicial authorities.

5-3 If financial and non-financial institutions are required, pursuant to the provisions of this Law, to maintain any transaction or account records beyond the minimum time required by the law, they shall keep the original records or documents until the conclusion of the time specified in the request.

Article (6):
Financial and non-financial institutions shall establish precautionary and internal monitoring measures to uncover and foil any of the crimes provided for in this Law and comply with the instructions issued by the competent monitoring authorities in this field.

6-1 The competent monitoring authorities shall set and develop the appropriate regulatory instructions and rules to be applied against the crimes prescribed by law, and the means and controls necessary to ensure compliance of financial and non-financial institutions with laws, rules and regulations to combat money laundering and the financing of terrorism.

6-2 Precautionary and internal monitoring measures established by the financial and non-financial institutions to uncover the crimes provided for in this Article, shall include the following:

(a) Setting written and effective controls to prevent exploitation of those institutions in money laundering transactions and/or the financing of terrorism and to assist in uncovering suspicious transactions, and to prevent the misuse of technological developments in money laundering or terrorism financing schemes, and to address and

manage the risks associated with non-face to face business relationships or transactions.

(b) Ensuring that the instructions issued by the monitoring authority are the minimum applicable instructions.

(c) Following up and monitoring to ensure application of instructions and adequacy of measures.

(d) Updating such controls periodically in line with developments in money laundering **or the financing of terrorism** activities.

Article (7):

Upon availability of sufficient indications and evidence showing that a complex, an immense or an unusual deal or transaction has been made, or that an activity of suspicious nature or purpose is underway, or is related to money laundering, financing terrorism, terrorist acts, or terrorist organizations, financial and non-financial institutions shall promptly take the following measures:

(a) Immediately report said transaction to Financial Intelligence Unit provided for in Article (11) of this Law.

(b) Prepare a report detailing all available data and information about such transactions and the parties involved, and provide the Intelligence Unit with such report.

7-1 Financial and non-financial institutions shall establish indicators of suspicion of money laundering or the financing of terrorism. They shall continuously update such indicators to keep up with developments and diversification of means for conducting such transactions while complying with instructions issued by monitoring agencies in that regard, and to pay special attention to unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

7-2 financial institutions and non-financial institutions are required to report to the Financial Intelligence Unit all suspicious transactions, including any attempts to carry out such transactions.

7-3 Notification of the Financial Intelligence Unit shall be according to the form approved by the Unit, provided that the notification shall include the following information at a minimum:

(a) Names of the accused, information about their addresses and telephone numbers.
(b) A statement of the suspicious transaction, parties involved, circumstances of its discovery and its current status.
(c) Determining the amount subject of the suspected transaction and relevant banking or investment accounts.
(d) Reasons and causes for suspicion upon which the reporting officer relied.

7-3 The report prepared by the financial and non-financial institutions regarding reported transactions shall observe the following:

(a) Financial institutions shall submit the report to the Financial Intelligence Unit within ten days from the date of notification, provided that it includes the following:

- Account statements for a period of six months.
- Copies of the documents attached to the documents for opening the account.
- Data related to the nature of the transactions reported.
- Indications and justifications for suspicion along with supporting documents.

(b) When requested by the Unit, non-financial institutions shall submit their reports on the notifications within two weeks from the date of request. The request may include the following:

- Information on the reported party.
- Statement of the business or financial transactions concerning the reported person or the related parties.
- Submission of indications and grounds for suspicion together with supporting documents.

Article (8):
As an exception to the provisions concerning banking confidentiality, financial and non-financial institutions shall submit documents, records and information to the judicial or competent authority upon request.

8-1 The judicial authority or the Bureau of Investigation and Public Prosecution or the Financial Intelligence Unit shall request the documents, records, and information from the financial and non-financial institutions through the Anti-Money Laundering Unit at the Saudi Arabian Monetary Agency for financial institutions under its supervision, through the Anti-Money Laundering Unit at the Ministry of Commerce and Industry for non-financial institutions, and through the Anti-Money Laundering Unit at the Capital Market Authority for stock exchange transactions and institutions under its supervision, and through the Ministry of Justice for fixed properties.

8-2 All documents, records and information shall be promptly submitted by financial and non-financial institutions to the judicial authority or the Bureau of Investigation and Public Prosecution or the Financial Intelligence Unit, upon request, through the Anti-Money Laundering Unit at the Saudi Arabian Monetary Agency for the financial institutions under its supervision, and through the Anti-Money Laundering Unit at the Ministry of Commerce and Industry for the non-financial institutions, and through the Anti-Money Laundering Unit at the Capital Market Authority for stock exchange transactions and institutions under its supervision, and through the Ministry of Justice for fixed properties.

8-3 Financial and non-financial institutions may not use the principle of confidentiality of accounts, identity of clients or information recorded pursuant to any other law as a pretext for withholding information.

Article (9):
Financial and non-financial institutions as well as their staff and others subject to the provisions of this Law shall not alert clients or allow for their alert or alert other related parties of suspicions regarding their activities.

9-1 In implementing this Article and in order to avoid any act that may alert clients or others, the following shall be observed:

(a) Formal acceptance of transactions from clients and not rejecting them for appearing unusual or suspicious.
(b) Avoiding suggesting alternatives to clients or providing them with advice or counsel in order to avoid instructions concerning the transactions conducted.
(c) Keeping confidential reporting of transactions or clients or related information to the Financial intelligence Unit .
(d) Communication with clients or foreign parties to inquire about the nature of the transactions shall not lead to suspicions.
(e) Not informing clients that their transactions are under review or monitoring or the like.

Article (10):

Financial and non-financial institutions shall introduce programs for Anti-Money laundering transactions, provided that said programs include the following as a minimum:

(a) Developing and implementing policies, plans, procedures and internal controls, including appointment of qualified officers at the higher administrative level to implement the same.
(b) Setting up internal audit and control systems to ensure that basic requirements for combating money laundering are in place.
(c) Setting up continuing training programs for employees concerned, to acquaint them with the latest developments in the field of money laundering transactions and to improve their abilities to recognize such transactions, their patterns and ways of combating them.

10-1 The director general or whoever he authorizes in the financial and non-financial institutions shall be responsible for implementing and developing policies, plans, procedures and internal controls pertaining to combating money laundering or terrorist financing.

10-2 Financial and non-financial institutions shall designate an employee or a department to be responsible for reporting and communicating with the Financial Intelligence Unit provided for in Article (11) of this Law. With regard to small non-financial sole proprietorships, reporting shall be directly made by the establishment owner or whoever he authorizes.

10-3 Financial and non-financial institutions shall establish a monitoring unit for conducting monitoring programs and internal audit in the field of combating money laundering or terrorist financing, provided that the task of the external auditor, if any, shall include a special program to ensure the extent of adherence of the financial and non-financial institutions to the polices of combating money laundering or terrorist financing.

10-4 Financial and non-financial institutions shall seek the assistance of the competent monitoring authorities when introducing means to ensure adherence to laws, regulations, and rules prescribed for combating money laundering or terrorist financing.

10-5 Financial and non-financial institutions shall set up plans, and programs and allocate budgets for training and qualifying their staff in the field of combating money laundering or terrorist financing according to the size and activity of such institutions, in coordination with the relevant monitoring authorities.

10-6 Assistance of specialized domestic and foreign institutions shall be sought in implementing the preparation, qualification and training programs in the field of combating money laundering or terrorist financing. Said training programs shall cover the following:

(a) Agreements, laws, rules and instructions related to combating money laundering or terrorist financing.
(b) Policies and laws of the monitoring authorities in the field of combating money laundering or terrorist financing.
(c) New developments in the field of money laundering transactions and terrorist financing and other suspicious transactions and ways of recognizing such transactions, their patterns, and ways of combating them.
(d) Civil and criminal liability of each employee pursuant to the pertinent laws, regulations and instructions.

Article (11):
A unit for combating money laundering shall be established under the name of "Financial Intelligence Unit". Its responsibilities shall include receiving notifications, analyzing them and preparing reports regarding suspicious transactions in all financial and non-financial institutions. The Implementing Regulations of this Law shall specify the seat of this Unit, its formation, powers, method of discharging its duties as well as to whom it reports.

11-1 The Unit's seat and to whom it reports:
The Unit shall report to the Assistant to the Minister of Interior for Security Affairs. Its main seat shall be in the city of Riyadh. It may have branches in different parts of the Kingdom.

11-2 Formation of the Unit:
It shall be formed of a chairman and an assistant and a sufficient number of specialists in money laundering crimes or terrorist financing, in the financial, accounting, legal, computer and security fields.

11-3 Jurisdiction of the Unit:
The Unit shall have power to:

(a) Receive notifications from financial and non-financial institutions and other government agencies and individuals concerning transactions suspected of being money laundering or terrorist financing crimes.
(b) Create a database to be provided with all reports and information related to money laundering or terrorist financing. This database shall be regularly updated, kept confidential. and make them available to competent authorities.
(c) Request and exchange information with related agencies and take the necessary measures to combat money laundering or terrorist financing.

(d) Request and exchange information with other financial investigation units with respect to combating money laundering or terrorist financing, pursuant to Article (22) of this Law.

(e) Prepare the forms used by financial and non-financial institutions in reporting transactions suspected of money laundering or terrorist financing. Such forms shall include data that assist the Unit in gathering information, analysis, investigation, entering them in the database and updating them if necessary.

(f) Gather information on reports it receives about transactions suspected to be money laundering or terrorist financing. The Unit may seek the assistance of necessary experts and specialists from agencies concerned.

(g) The Financial Intelligence Unit shall conduct field investigation and inquiry and may request the same from the security sectors at the Ministry of Interior. In the presence of sufficient evidence that the transactions reported are related to money laundering or terrorist financing, it shall refer them to the agency in charge of investigation and prepare a detailed report providing sufficient data about the committed crime, the culprit(s) and the nature of such evidence, accompanied by the opinion, together with all relevant documents and information.

(h) Request the Bureau of Investigation and public Prosecution to carry out the preventive seizure of funds, properties and means relating to a money laundering or terrorist financing crime as provided for in Article (12) of this Law.

(i) Take action with regard to reports, and information where information gathering and analysis indicate the absence of evidence or suspicion of the commission of any of the acts provided for in Article (2) of this Law.

(j) Coordinate with the authorities monitoring financial and non-financial institutions to make available means necessary to verify the adherence of such institutions to the laws, regulations and instructions prescribed for combating money laundering or terrorist financing.

(k) Provide feedback to financial and non-financial institutions reporting and to the competent authorities with combating money laundering and terrorist financing.

(l) Participate in organizing awareness programs on combating money laundering or terrorist financing, in coordination with the Permanent Committee for Combating Money Laundering.

(m) Submit necessary recommendations to the Permanent Committee for Combating Money Laundering about the difficulties and suggestions in the field of combating money laundering or terrorist financing.

(n) The Financial Intelligence Unit may enter into memorandums of understanding with other financial investigation units pursuant to applicable laws and procedures.

(o) Take necessary legal procedures to join the Financial Investigation Units Group (The Egmont Group).

11-4 Departments of the Unit:

The Unit shall be composed of the following departments:

(a) Department of Reports.

(b) Department of Information Gathering and Analysis

(c) Department of Information Exchange.

(d) Department of Information and Studies.

First: Department of Reports:

(1) Receiving reports on dubious and suspicious transactions regarding their nature and purpose or that they relate to money laundering or terrorist financing.

(2) Receiving reports by fax or any other means. In case of telephone reports, they shall be confirmed as soon as possible in any written form.

(3) Receiving reports shall be in the form prepared by the Unit and provided to all related departments and financial and non-financial institutions.

(4) Recording the reports in special records with serial numbers, under which all necessary information is entered.

(5) Referring reports to the Department of Information Gathering and Analysis to determine the existence of suspicion and indications of a money laundering or terrorist financing crime.

Second: Department of Information Gathering and Analysis:

(1) Ensuring that the report includes the necessary information as well as attaching documents necessary for analysis.

(2) Requesting the relevant agency to provide information, reports, documents needed for analysis when necessary.

(3) Reviewing data and information included in the report and comparing them with information available to the Department to verify their accuracy and assess their appropriateness, making use of records of security, financial, commercial and other related agencies.

(4) In the presence of sufficient indications that the transactions stated in the report are related to money laundering or terrorist financing, and a need arises for field investigations or the arrest of persons or tracking funds or assets under suspicion, the Unit shall do so. It may request the relevant security agencies in charge of investigation and inquiry at the Ministry of Interior to do the same. Hence, prepare an analytical report including their views, accompanied by the relevant report, and documents to complete the procedures and refer it to the agency in charge of investigation.

(5) Requesting the Bureau of Investigation and public Prosecution to carry out preventive seizure of funds, properties, and means related to a crime of money laundering as stipulated in Article (12) of this Law.

(6) Deal with reports and information, where information gathering and analysis indicate the absence of evidence or suspicion of the commission of any of the acts provided for in Article (2) of this Law.

Third: Department of Information Exchange and Follow up:

(1) Exchange of information with domestic authorities and similar units in foreign countries with respect to combating money laundering or terrorist financing.

(2) Providing the Department of Information and Studies with the number of requests received by the Department periodically every month, whether domestic or foreign.

Fourth: Department of Information and Studies:

(1) Creating a database for the following:

(a) Reports on suspicious transactions received and analyzed and traced.

(b) Reports referred to security agencies to complete the investigation and inquiry procedures or to the competent investigation agency.
(c) Reports leading to judicial or administrative action.
(d) Convictions in money laundering or terrorist financing cases.
(e) Requests for exchange of information received by the Unit from local authorities and foreign counterparts.
(f) Number of reports shelved and grounds thereof.

(2) Monitoring indicators of money laundering or terrorist financing crimes in financial and non-financial institutions and ways of perpetrating them as well as proposing solutions and measures to be taken for combating them and referring the same to the Permanent Committee for Combating Money Laundering.
(3) Preparing an annual report on the unit's work and forwarding it to the Minister of Interior as well as providing the Permanent Committee for Combating of Money Laundering with a copy thereof.
(4) Keeping apprised of recent developments related to money laundering or terrorist financing crimes through relevant regional and international organizations and commissions.
(5) Participating in organizing awareness programs with respect to combating money laundering or terrorist financing, in coordination with the Permanent Committee for Combating Money Laundering.

Article (12):
The Financial Intelligence Unit upon establishment of suspicion, shall request the authority in charge of investigation to carry out preventive seizure to the funds, properties and means associated with a money laundering crime, for a period not exceeding twenty days. Should there be a need for the preventive seizure to continue for a longer period, it shall be pursuant to a judicial order from the court of competent jurisdiction.

12-1 The preventive seizure shall take place on all funds, properties or means owed to the suspect(s) and are in the possession of individuals, companies, financial and non-financial institutions or any other entity.

12-2 The request for preventive seizure shall be issued by the Head of Financial Investigation Unit or whoever he deputizes.

12-3 The preventive seizure request shall be made by a memorandum that includes a full statement of the following:

(a) Detailed information of the persons whose funds, properties or means to be seized.
(b) Specification of funds, properties and means to be seized.
(c) Suspicions, recitals and confirmed reasons supporting the seizure.
(d) Duration of the preventive seizure shall not exceed the period stated in this Article.

12-4 The request for preventive seizure shall be sent in an appropriate confidential manner to the Bureau of Investigation and Public Prosecution. The request for seizure shall be promptly acted on, and the Financial Investigation Unit shall be notified of the decision within 48 hours.

12-5 The period of the preventive seizure specified in this Article shall start from the date of its imposition.

12-6 Upon issuance of the approval of the Bureau of Investigation and Public Prosecution of the request of the Financial Intelligence Unit, the Unit of combating money laundering at the Saudi Arabian Monetary Agency shall be addressed to seize funds deposited in financial institutions, the Ministry of Commerce and Industry to seize properties and whatever relates to the activities of non-financial institutions, the Ministry of Justice to seize lands and real estate, the Directorate of Public Security to seize means, the Customs Authority to seize goods and means under its control and the Capital Market Authority to seize securities. The Financial Intelligence Unit shall be notified thereof.

12-7 Procedures regarding the request or an order for continuation of seizure shall be taken before the end of the twenty- day period by a sufficient time.

12-8 The investigation authority, upon issuance of an order for continuation of the preventive seizure, shall inform the monitoring

and security agencies to enforce the court order and notify the financial Intelligence Unit thereof.

12-9 If the authority in charge of the investigation deems that it is not necessary to impose preventive seizure on funds, properties and means, mentioned in the request submitted by the Unit, such authority shall promptly notify the Unit in writing of its disapproval of such request, giving its views thereon.

12-10 The monitoring agencies and authorities in charge of combating money laundering may request through the Financial Intelligence Unit the imposition of the preventive seizure in compliance with the period specified in the Law.

12-11 The request for the continuation of the preventive seizure shall be through a petition deposited with the court, including the following:

(a) The court with which the lawsuit is filed.
(b) Date of submission of request.
(c) Subject of the lawsuit and what is requested by the public prosecutor and supporting evidence.
(d) The requested duration of seizure.
(e)

Article (13):

Information disclosed by financial and non-financial institutions may be exchanged, according to the provisions of Article (8) of this Law between these institutions and the competent authorities, should such information be related to a violation of the provisions of this Law. The competent authorities shall observe the confidentiality of such information and not disclose it, except as necessary for use in investigations or lawsuits related to the violation of the provisions of this Law.

Article (14):
The Implementing Regulations of this Law shall determine the rules and procedures of disclosure of cash amounts and precious metals permitted to enter or leave the Kingdom and shall determine the amounts of money and weights required to be disclosed.

14-1 Estimated cash or financial instruments negotiated by the bearer or precious metals that must be disclosed when leaving or entering the Kingdom of "60.000" sixty thousand riyals or its equivalent in foreign currency.

14-2 prevent exit or entry of any traveler cash or financial instruments of negotiable bearer or precious metals exceeding the limit without the mobilization model disclosure in the case of controlling the security authorities, customs or the amount of financial instruments or negotiable bearer or precious metals that have not And disclosed more than the limit referred to the customs (the official) to investigate the reasons for non-disclosure if the reasons for his conviction required the mobilization of the passenger model disclosure and complete the remaining procedures for disclosure and allowed to leave or enter, including him, but in the absence of belief in the customs official reasons Or suspected money laundering or the financing of terrorism reference is the traveler to the competent authority for investigation and to inform the Financial Intelligence Unit to do so.

14-3 in the event of the outgoing passenger carrying precious metals worth more than sixty thousand riyals and wished to remove them from Saudi Customs shall review the disclosure by a performing seal and model disclosure and bill the purchase to ensure their value and if they applied for commercial purposes right the Unified Customs Law and its implementing regulations.

14-4 in the seizure of the outgoing passenger next to the Kingdom or in cases of repeated or not releasing in the event of releasing the relationship of suspicion and generate funds out suspicious money laundering or financing terrorism or providing false statements about him disclosure of cash or financial instruments that can be converted or precious metals over Value limit and be prepared record by the officer, which shall refer it to Customs and the Customs and then transmitted to the competent authority to investigate the claim to punish him according to article "20" of the anti-money laundering regime or the customs system, as is clear from the investigation and notify the Financial

Intelligence Unit and the excess amount shall be deposited The limit by customs in a special account secretariats and precious metals are impounded by Customs pending the receipt of a signal from the investigation.

14-5 customs inspections on the basis of a random sample or provide information on the suspected money laundering or the financing of terrorism and out of control for cash or financial instruments negotiable bearer or precious metals.

14-6 unveiled at next to Saudi customs officer to get him to cash or financial instruments of negotiable bearer or precious metals worth more than the limit For the customs officer in the port to ensure the safety of cash from counterfeiting by the representative of SAMA, and for precious metals It is required to prove ownership under the invoice and if it finds it for commercial purposes is administered by the Unified Customs Law and its implementing regulations.

14-7 send a copy of the information disclosure forms as agreed upon by the Customs Department of Financial Intelligence Unit set forth in the article "11" from the system of checking people from a crime of money laundering or terrorist financing or any other crimes.

14-8 review in the absence of owners of these funds or precious metals after the expiration of the period of "90" ninety days treated in accordance with applicable regulations seizures.

14-9 these procedures apply to companies or financial institutions and non-financial and gold shops and missions of the Hajj and Umrah and service companies for the transfer of cash or postal parcels and other postal and missions while maintaining its right to exercise its work.

14-10 Customs Department to develop a database of names of persons who had previously disclosed or not to know the purpose of which is repeated with the notice of the Financial Intelligence Unit.

14-11 Customs prepare the model disclosure referred to in this article after coordination with the Financial Intelligence Unit and distribution outlets.

14-12 The Ministry of the Interior and the Ministry of Finance to report such actions necessary instructions to various means available and provide guidance

in several paintings prominently at the entry and exit points around pointing out the procedures and sanctions to be applied in case of violating the order.

Article (15):
If a judgment to confiscate funds, proceeds or means is rendered pursuant to the provisions of this Law, and they are not required to be destroyed, the competent authority shall dispose of them according to the law or share them with countries which are parties, with the Kingdom, to agreements or treaties in force.

15-1 The competent authority provided for in this Article and which is in charge of disposal of confiscated funds, proceeds and means is the authority enforcing the preventive seizure.

15-2 The competent authority provided for in this Article and which is in charge of sharing confiscated funds, proceeds and means with countries that are parties with the Kingdom to agreements or treaties in force is the Mutual Legal Assistance at the Ministry of Interior.

15-3 The request for confiscation of funds, proceeds or means shall be stated in the prosecution's accusatory pleading and in the judicial judgments rendered by the courts in this regard.

15-4 The confiscation judgment shall include funds, proceeds or means subject of the crime, whether seized or not seized inside or outside the country.

15-5 In implementing this Article regarding funds, proceeds or means confiscated pursuant to a judgment, the following shall be observed:

(a) Article (94) of the Law of Criminal Procedures and its Implementing Regulations regarding materials that perish over time or the preserving of which requires huge expenses that consume its value.

(b) Depositing confiscated funds, proceeds or means with the state treasury.

(c) The Council of Ministers' Resolution No. (47) dated 28/1/1421H providing for the transfer, to an independent account at the Saudi Arabian Monetary Agency, of funds seized in the possession of the accused in drug cases and the value of materials regarding which confiscation judgments were rendered. Funds in said account shall be used towards covering the needs of the General Directorate for Combating Drugs.

Article (16):

Anyone who commits a crime of money laundering, as provided for in Article (2) of this Law, shall be subject to imprisonment for a period not exceeding (10) years and a fine not exceeding five million riyals, or by either punishment, along with the confiscation of funds, proceeds and means subject of the crime. Should the funds and proceeds mix with funds acquired from legitimate sources, said funds shall be subject to confiscation within limits equal to the estimated value of the illegal proceeds.

The competent court may exempt from these punishments the owner, possessor, or user of the funds or proceeds subject of incrimination, if he notifies the authorities prior to their knowledge of the sources of the funds or proceeds and the identity of accomplices, without him benefiting from their revenues.

16-1 The investigating authority shall assess the estimated value of the illegal proceeds by seeking the assistance of experts. A judgment from a competent court shall be rendered in this regard.

16-2 Request for consideration of exemption from punishments of the notifying person shall be made by the authority in charge of investigation.

16-3 Upon receiving such notifications, procedures for investigation and inquiry shall be taken so as to ensure that the authorities have no knowledge of the crime.

Article (17):

The punishment of imprisonment shall be for a period not exceeding fifteen years and a fine not exceeding seven million Saudi riyals, if the money laundering crime is coupled with one of the following cases:

(a) The perpetrator's committing the crime through an organized crime syndicate.
(b) The perpetrator's use of violence or weapons.
(c) The perpetrator's holding of a public post to which the crime is connected or exploiting his authorities or influence in the commission of the crime.
(d) Deceiving or exploiting women and minors.
(e) Committing the crime through a correctional, charitable or educational institution or in a social service facility.
(f) Issuance of previous domestic or foreign judgments convicting the perpetrator, especially for similar crimes.

Article (18):

Without prejudice to other laws, any chairman of the board of directors of financial and non-financial institutions, board member, owner, manager, employee, authorized representative, or hired hand acting in these capacities, who fails to fulfill any of the obligations provided for in Articles (4, 5, 6, 7 ,8, 9 and 10) of this Law shall be subject to imprisonment for a period not exceeding two years and a fine not exceeding five hundred thousand riyals or by either punishment. The punishment shall apply to those engaging in the activity without obtaining the required licenses.

18-1 In this Article, "other laws" means all laws issued by agencies monitoring financial and non- financial institutions, such as Companies Law, Law of Commercial Register, Banks Monitoring Law and the Capital market law.. etc.

Article (19):
Pursuant to a judgment based upon a petition submitted by the competent authority, a fine of not less than one hundred thousand riyals and not exceeding the value of funds subject to the crime may be imposed on financial and non-financial institutions whose liability is proven pursuant to the provisions of Articles (2) and (3) of this Law.

19-1 The competent authority in this Article is the Bureau of Investigation and Public Prosecution.

19-2 The liability lawsuit of financial and non-financial institutions shall be based on technical reports issued by the monitoring agencies in addition to other proving methods.

19-3 Application of punishments provided for in this Article shall not conflict with administrative or disciplinary penalties provided for in other laws which may be imposed on financial and non- financial institutions by the monitoring agencies with regard to establishing their liability.

Article (20):
With the exception of punishments provided for in this Law, anyone violating its provisions shall be subject to imprisonment for a period not exceeding six months and a fine not exceeding one hundred thousand riyals, or by either punishment.

Article (21):
The punishments specified in this Law shall not apply to those who violate it in good faith.

21-1 Good faith shall be determined by the competent judicial authority and shall be inferred from the objective conditions and circumstances.

Article (22):
Information disclosed by financial and non-financial institutions may be exchanged between those institutions and the competent authorities in other countries which are parties, with the Kingdom, to agreements and treaties in force or on the basis of reciprocal treatment, pursuant to established legal procedures, provided that this shall not prejudice the provisions and practices related to the confidentiality of financial and non-financial institutions.

22-1 Competent authorities in other countries provided for in this Article refer to the Financial Intelligence Unit or its equivalent in terms of functions.

22-2 Information disclosed by the financial and non financial institutions concerning a money laundering or terrorist financing crime shall be exchanged through the Financial Intelligence Unit.

22-3 When exchanging information pursuant to the provisions of agreements and treaties in effect or on the basis of reciprocal treatment, the following shall be observed:

(a) Information exchanged shall only be used for the purpose it is requested for.
(b) Information exchanged shall not be disclosed to a third party except with the approval of the Financial Intelligence Unit.

Article (23):
Upon request from a court or a competent authority in another country which is a party with the Kingdom to an agreement or treaty in force or on the basis of reciprocity, the judicial authority may order seizure of funds, proceeds or means related to a money laundering crime, according to the laws in force in the Kingdom.
Upon request from a competent authority in another country, which is a party with the Kingdom to an agreement or treaty in force or on the basis of reciprocity, the competent authority may order tracing of funds, proceeds or means associated with a money laundering crime, according to laws in force in the Kingdom.

23-1 Requests received from other countries regarding seizure or tracing of funds, proceeds or means related to money laundering or terrorist financing crime, shall be deemed one of the functions of the Mutual legal Assistance Committee based in the Ministry of the Interior and problem resolution by the Council of Ministers (No. 168) in e 11/8/1419 Amended Resolution No. (3) 7/1/1424 e, and legal procedures shall be taken in such a matter.

23-2 Requests related to seizure of funds, proceeds or means regarding money laundering crime, shall be referred to the Board of Grievances to render the judicial judgments for implementation by the competent monitoring agencies. The Financial Investigation Unit shall be informed thereof.

23-3 Requests related to tracing of funds, proceeds or means regarding a money laundering or terrorist financing crime shall be referred to the Bureau of Investigation and Public Prosecution, for implementation by the competent monitoring agencies.

23-4 Any request submitted pursuant to this Article shall include the following:

(a) Specifying the entity submitting the request.
(b) Subject and nature of the investigation, tracing, or the judicial procedures to which the request relates, as well as the name and jurisdiction of the authority conducting these investigations, tracing or judicial procedures.
(c) A summary of relevant facts and the procedures taken.
(d) Specifying the type of request or any special procedure, which the requesting party wishes to be traced.
(e) Specifying the identity of any person concerned, his location and nationality.
(f) Specifying the funds, proceeds and means required to be seized or traced.
(g) Specifying the requested duration of seizure.
(h) Proof of judicial jurisdiction of the requesting country.

Article (24):
Any final judicial judgment providing for the confiscation of funds, revenues or means related to money laundering crimes, rendered by a competent court in another country, which is a party with the Kingdom, to an agreement or treaty in force or on the basis of reciprocity, may be recognized and enforced if the funds, proceeds or means provided for in this judgment may be subject to confiscation in accordance with the applicable law in the Kingdom.

24-1 Requests for execution of judgments received from other countries in relation to a money laundering or terrorist financing crime shall be deemed part of the functions of the Mutual legal Assistance Committee.

24-2 Requests related to execution of foreign judgments relating to a money laundering crime shall be referred to the Board of Grievances.

24-3 Any judgment to be recognized and executed shall include, in addition to paragraphs from (a) to (h) of Article 23-6 of these Regulations, the following:

(a) Confiscation shall be pursuant to an enforceable final judicial judgment in one of the crimes provided for in Article (2) of this Law.
(b) The confiscation judgment shall be enforceable in the Kingdom.
(c) Funds or proceeds to be confiscated may not have been previously subject of the confiscation as a result of another judicial judgment or by a competent authority.

Article (25):
Chairmen of the boards of directors of financial and non-financial institutions, board members, owners, employees, hired hands or their authorized representatives, shall be exempted from criminal, civil or administrative liability which may result from the performance of the duties provided for in this Law or upon violation of any restriction imposed to ensure confidentiality of information, unless their actions are proven to be in bad faith, with the intent to harm the person conducting the transaction.

25-1 Bad faith shall be determined by the competent judicial authority and shall be inferred from the factual or objective and circumstances.

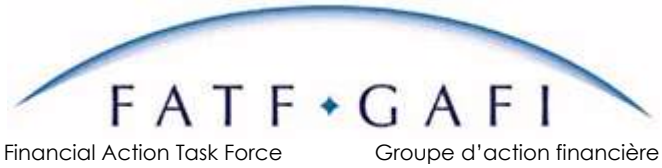
Article (26):
General courts shall have jurisdiction to decide all crimes provided for in this Law.

Article (27):
The Bureau of Investigation and Public Prosecution shall investigate and prosecute before general courts crimes provided for in this Law.

Article (28):
The Minister of Interior, in coordination with the Minister of Finance and National Economy, shall issue the Implementing Regulations of this Law within ninety days from the date of its issuance.

28-1 The Implementing Regulations shall be reviewed for the purpose of updating within five years or when necessary.

Article (29):
This Law shall be published in the Official Gazette and shall be effective sixty days from the date of its publication.



FATF Reference Document

Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations

27 February 2004
(Updated as of February 2009)

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

Table of Contents

Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations

Anti-Money Laundering/Combating Terrorist Financing Methodology 2004 (Updated as of February 2009)

Introduction

This document consists of three sections. Following this introduction, the first section consists of an overview of the assessment methodology, its background, how it will be used in evaluations/assessments, and a description of what is necessary for an effective anti-money laundering and combating the financing of terrorism ("AML/CFT") system. The second section contains guidance and interpretation concerning the Methodology, including on the essential criteria, the additional elements and on compliance. The third section sets out the essential criteria and the additional elements for each of the FATF Recommendations. Finally, there is annex to the Methodology that sets out definitions or meanings for many of the words or phrases that are used in the document.

The AML/CFT Assessment Methodology

Background to Methodology

1. The Anti-Money Laundering/Combating Terrorist Financing (AML/CFT) Methodology 2004, including the assessment criteria, is designed to guide the assessment of a country's compliance with the international AML/CFT standards as contained in the FATF Forty Recommendations 2003 (updated as of October 2004) and the FATF Nine Special Recommendations on Terrorist Financing 2001 (updated as of February 2008) (referred to jointly as the FATF Recommendations). The criteria within this Methodology do not expand upon or modify the Forty Recommendations and Nine Recommendations which constitute the international standard. The Methodology is a key tool to assist assessors when they are preparing AML/CFT detailed assessment reports/mutual evaluation reports. It will assist them in identifying the systems and mechanisms developed by countries with diverse legal, regulatory and financial frameworks, in order to implement robust AML/CFT systems. The Methodology is also useful for countries that are reviewing their own systems, including in relation to technical assistance projects.

2. It reflects the principles set out in the FATF Recommendations. It is also informed by the experience of the FATF and the FATF-style regional bodies (FSRBs) from their mutual evaluations, of the International Monetary Fund (the Fund) and the World Bank (the Bank) in the Financial Sector Assessment Program and by the Fund from the Offshore Financial Center assessment program. The FATF, the Fund and the Bank have also reviewed the assessments/mutual evaluations conducted in 2002 and 2003 using the AML/CFT Methodology issued in October 2002, and these reviews have also provided guidance in developing this Methodology.

Evaluations/assessments using the Methodology

3. The Methodology follows the structure of the FATF Recommendations. However, as the Methodology is a tool to assist assessors in determining whether countries are in compliance with the FATF Recommendations, it is not intended that detailed assessment reports/mutual evaluation reports will rigidly follow the format and structure of the Methodology. Rather the format for these reports will be based on the four fundamental areas noted in paragraph 6 below.

4. The assessments will also need to be based on and refer to relevant underlying information, such as the quantum and type of predicate offences for money laundering; the vulnerability of the country to money laundering or terrorist financing, the methods, techniques and trends used to launder money or fund terrorists; the structure of the financial system and the nature of the sectors dealing with designated non-financial businesses and professions; the nature of the underlying criminal justice system, as well as any changes that have been made to the AML/CFT system in the relevant period. Most importantly, the reports will allow for an assessment of whether the Recommendations have been fully and properly implemented and the AML/CFT system is effective. As in previous FATF evaluation rounds, this could be judged by reference to quantitative data and the results that have been achieved, or could be based upon more qualitative factors.

5. It should be noted that in some countries, AML/CFT issues are matters that are addressed not just at the level of the national government, but also at state/province or local levels. For example, profit generating criminal offences may exist at both federal and state levels. Measures to combat money laundering should be taken at the appropriate level of government, necessary to ensure that the full range of AML/CFT measures applies. When evaluations or assessments are being conducted, appropriate steps should be taken to ensure that AML/CFT measures at the state/provincial level are also adequately addressed.

Structure necessary for an effective AML/CFT system

6. An effective AML/CFT system requires an adequate legal and institutional framework, which should include: (i) laws that create money laundering (ML) and terrorist financing (FT) offences and provide for the freezing, seizing and confiscation of the proceeds of crime and terrorist funding; (ii) laws, regulations or in certain circumstances other enforceable means that impose the required obligations on financial institutions and designated non-financial businesses and professions; (iii) an appropriate institutional or administrative framework, and laws that provide competent authorities with the necessary duties, powers and sanctions; and (iv) laws and other measures that give a country the ability to provide the widest range of international co-operation. It is also essential that the competent authorities ensure that the whole system is effectively implemented. The assessment of individual recommendations, as well as any findings relevant to paragraph 7 below, may lead to broader conclusions on the global effectiveness of a country's AML/CFT system. These conclusions should be mentioned in both the mutual evaluation report/detailed assessment report and in the executive summary as part of the report's overall findings on the AML/CFT system in the country and the effectiveness of that system (see also the MER template in the Handbook for Countries and Assessors).

7. An effective AML/CFT system also requires that certain structural elements, not covered by the AML/CFT assessment criteria, be in place. The lack of such elements, or significant weaknesses or shortcomings in the general framework, may significantly impair the implementation of an effective AML/CFT framework. Although the AML/CFT assessment criteria do not cover these conditions, assessors should consider whether there are apparent major weaknesses or shortcomings and should note these in the mutual evaluation/detailed assessment report. These elements should include in particular:

a) the respect of principles such as transparency and good governance;
b) a proper culture of AML/CFT compliance shared and reinforced by government, financial institutions, designated non-financial businesses and professions; industry trade groups, and self-regulatory organisations (SROs);
c) appropriate measures to prevent and combat corruption, including, where information is available, laws and other relevant measures, the jurisdiction's participation in regional or international anti-corruption initiatives (such as the United Nations Convention against

Corruption[1]) and the impact of these measures on the jurisdiction's AML/CFT implementation;

d) a reasonably efficient court system that ensures that judicial decisions are properly enforced;

e) high ethical and professional requirements for police officers, prosecutors, judges, etc. and measures and mechanisms to ensure these are observed;

f) a system for ensuring the ethical and professional behaviour on the part of professionals such as accountants and auditors, and lawyers. This may include the existence of codes of conduct and good practices, as well as methods to ensure compliance such as registration, licensing, and supervision or oversight.

Guidance on the Essential Criteria, the Additional Elements, and the Compliance Ratings, and General Interpretation concerning the AML/CFT Standards and Methodology

8. The assessment of the adequacy of a country's AML/CFT framework will not be an exact process, and the vulnerabilities and risks that each country has in relation to ML and FT will be different depending on domestic and international circumstances. ML and FT techniques evolve over time, and therefore AML/CFT policies and best practices will also need to develop and adapt to counter the new threats.

9. The FATF Recommendations provide the international standard for combating money laundering and terrorist financing and the Recommendations and the criteria set out in this Methodology are applicable to all countries. However, assessors should be aware that the legislative, institutional and supervisory framework for AML/CFT may differ from one country to the next. Provided the FATF Recommendations are complied with, it is acceptable that countries implement the international standards in a manner consistent with their national legislative and institutional systems, even though the methods by which compliance is achieved may differ. In this regard, assessors should be aware of each country's stage of economic development, its range of administrative capacities, and different cultural and legal conditions. Moreover, the report should provide the context for the assessment, and make note of any progress that has been or is being made in implementing the international standards and the criteria in this Methodology.

Essential Criteria

10. The essential criteria are those elements that should be present in order to demonstrate full compliance with the mandatory elements of each of the Recommendations. Criteria to be assessed are numbered sequentially for each Recommendation, but the sequence of criteria is not important. In some cases elaboration (indented below the criteria) is provided in order to assist in identifying important aspects of the assessment of the criteria. In addition, examples are provided, for some criteria, of situations in which a particular requirement could apply, or where there may be exceptions to the normally applicable obligations. The examples are not part of the criteria, and are only illustrative, but they may provide guidance as to whether national measures for particular criteria may be appropriate.

[1] Other initiatives include the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, the Group of States against Corruption (Groupe d'Etats contre la corruption—GRECO), the ADB/OECD Anti-Corruption Initiative for Asia/Pacific, the African Union Convention on Preventing and Combating Corruption, and the Inter-American Convention against Corruption.

Compliance Ratings

11. For each Recommendation there are four possible levels of compliance: compliant, largely compliant, partially compliant, and non-compliant. In exceptional circumstances a Recommendation may also be rated as not applicable. These ratings are based only on the essential criteria, and defined as follows:

Compliant	The Recommendation is fully observed with respect to all essential criteria.
Largely compliant	There are only minor shortcomings, with a large majority of the essential criteria being fully met.
Partially compliant	The country has taken some substantive action and complies with some of the essential criteria.
Non-compliant	There are major shortcomings, with a large majority of the essential criteria not being met.
Not applicable	A requirement or part of a requirement does not apply, due to the structural, legal or institutional features of a country e.g. a particular type of financial institution does not exist in that country.

12. Assessors should review whether the laws and regulations meet the appropriate standard and whether there is adequate capacity and implementation of those laws. Countries should only be regarded as fully complying with criteria if the relevant laws, regulations or other AML/CFT measures are in force and effect at the time of the on-site visit to the country or in the period immediately following the on-site mission, and before the finalisation of the report.

13. Laws that impose preventive AML/CFT requirements upon the banking, insurance, and securities sectors should be implemented and enforced through the supervisory process. In these sectors, the core supervisory principles issued by the Basel Committee, IAIS, and IOSCO should also be adhered to. For certain issues, these supervisory principles will overlap with or be complementary to the requirements set out in this Methodology. Assessors should be aware of, and have regard to any assessments or findings made with respect the Core Principles, or to other principles or standards issued by the supervisory standard-setting bodies. For other types of financial institutions, it will vary from country to country as to whether these laws and obligations are implemented and enforced through a regulatory or supervisory framework, or by other means.

Additional Elements

14. The additional elements are options that can further strengthen the AML/CFT system and may be desirable. They are derived from non-mandatory elements in the FATF Recommendations or from Best Practice and other guidance issued by the FATF, or by international standard-setters such as the Basel Committee on Banking Supervision. Although they form part of the overall assessment, they are not mandatory, and are not assessed for compliance purposes. To make this absolutely clear, the additional elements are formulated as questions. Assessors may consider and comment on the measures that have been taken or not taken, having regard to the particular circumstances of that country. In a similar way, assessors also have discretion to note other matters which they identify as strengthening or which might strengthen the AML/CFT system.

Effective Implementation

15. It is essential that all the FATF Recommendations are effectively implemented, and that assessments or evaluations address this issue and reflect it in the rating. The fundamental point, as noted in paragraphs 6 and 7 above, is that reports will not only assess formal compliance with the FATF Recommendations, but will also assess compliance having regard to whether the Recommendations have been implemented effectively. Assessors should regard effectiveness as an essential component in assessing each Recommendation. Effectiveness could have a positive, neutral, or negative influence on the overall rating for each Recommendation. The assessors' findings should be fully set out in the report. Assessors should note that the onus is on the assessed country to demonstrate (whether through statistics or by other factors) that implementation of the Recommendations is effective.

16. In the normal course of events, effective implementation of a particular Recommendation can only be measured against formal compliance with the criteria relating to that Recommendation (i.e. the requisite law, regulation or other enforceable means is in place and is being effectively implemented). However, in exceptional circumstances, when assessing the compliance of the country with those Recommendations that impose obligations on financial institutions, assessors may conclude that the objective of the Recommendations is being met, even in the absence of a structural framework that meets the strict FATF requirements. This may occur, for example, where financial institutions are complying with instructions or guidance ("drivers") issued by a competent authority, but where the "drivers" do not reach the level of other enforceable means.

17. Therefore, in exceptional circumstances, assessors may consider that an upgrade could be justified on the basis of effectiveness alone, provided that there is proven effectiveness, which reflects positive action taken by the authorities, and the following conditions apply:

- Any relevant "drivers" have been issued by a competent authority, and are understood within the jurisdiction to have directional effect, and which address the specific issues required under the essential criteria for the Recommendation, and;
- The competent authority routinely monitors for compliance with the "drivers"; has specific or general enforcement powers which may be invoked on the basis of non-compliance; and there is evidence that such powers have been used in such circumstances.

18. An upgrade of rating in these circumstances may only be considered from non-compliant to partially compliant, and the assessors must provide within the report a full analysis of the basis upon which such a decision was made.

19. When assessing whether particular Recommendations have been effectively implemented, assessors will need to take into account quantitative data and qualitative and other information. As noted in paragraph 9 above, it must be recognised that every country has different AML/CFT laws and systems and that each evaluation will always need to be assessed on its own merits. Judging effectiveness will also require assessors to be aware of the particular circumstances of an assessed country, including the ML and FT vulnerabilities and risks, the legal and institutional AML/CFT framework and the structural elements referred to in paragraphs 6 and 7 above. Consideration should also always be given to certain fundamental factors such as the population of the country, the size of its financial and DNFBP sectors, the amount and type of predicate crime and money laundering activity, and of vulnerability to terrorist financing etc. Absolute data is not usually determinative by itself, and should normally be considered relative to these other factors.

20. In addition to obtaining information on direct results and on the underlying context, assessors should also consider a range of other sources that may provide other relevant information on effectiveness such as reports by other bodies focused on similar or related issues including:

- country reports made under UNSCR 1373;

- FSAP or OFC reports issued by the IMF or World Bank
- reports on anti-bribery measures prepared by bodies such as the OECD or the GRECO committee of the Council of Europe;
- national studies on AML/CFT measures.

21. Another important element of the process for discussing and checking effectiveness is the on-site visit to the assessed country. The assessment team has the opportunity to obtain more detailed information from the various meetings that are held on-site, including in relation to ML and TF risks and vulnerabilities, and to cross check responses provided by government with the various associations and bodies from the private sector. Assessors should also note that it is permissible to use criteria from one recommendation to assess the effectiveness of implementation of other recommendations. For example, the resources available to an agency tasked to combat money laundering or terrorist financing (c.30.1), would usually also be relevant to the effectiveness of that agency e.g. financial supervisor body (R.23), FIU (R.26) etc.

General Interpretation and Guidance

22. A full set of definitions from the FATF Recommendations, together with some additional terms that are employed in this Methodology, are at Annex 1. Assessors should be fully familiar with the meaning of all these terms, and in particular those terms that are used throughout the Methodology, such as: *consider, country, designated non-financial businesses and professions (DNFBP), financial institutions, financing of terrorism (FT), legal persons and legal arrangements*. The term *financial institutions* is particularly fundamental to any AML/CFT assessment, and one of the starting points for all assessments will entail assessors developing a thorough understanding of the types of financial institutions that engage in the financial activities referred to in the definition. Assessors should also take note of the following guidance on other points of general interpretation, which is important to ensure consistency of approach.

23. **Risk of money laundering or terrorist financing** - For each Recommendation and each essential criteria where financial institutions should be required to take certain actions, assessors should normally assess compliance on the basis that all financial institutions should have to meet all the specified requirements. However, an important consideration underlying the FATF Recommendations is the degree of risk of money laundering or terrorist financing for particular types of financial institutions or for particular types of customers, products or transactions. A country may therefore take risk into account and may decide to limit the application of certain FATF Recommendations provided that either of the following conditions are met:

> (a) When a financial activity referred to in the definition of "financial institution" as defined in the Glossary is carried out on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring.
>
> (b) In other circumstances where there is a proven low risk of money laundering and terrorist financing, a country may decide not to apply some or all of the requirements in one or more Recommendations. However, this should only be done on a strictly limited and justified basis. For the purposes of this Methodology, assessors should be satisfied as to the adequacy of the process to determine low risk and the reasonableness of the conclusions.

24. In Recommendation 5 there are a number of criteria which allow countries to permit their financial institutions to take risk into account when determining the extent of the customer due diligence measures that the institution must take. This should not allow financial institutions to completely avoid doing the required measures, but could allow them to reduce or simplify the measures they have to take for certain criteria. Assessors need to be satisfied that there is an adequate mechanism by which competent authorities assess or review the procedures adopted by financial institutions to determine the

degree of risk and how they manage that risk, as well as to review the determinations made by institutions.

25. In Recommendations 5 and 9, reference is made to a financial institution being satisfied as to a matter. This also requires that the institution must be able to justify its assessment to competent authorities, and that assessors need to be satisfied that there is an adequate mechanism by which competent authorities can review the assessments of financial institutions.

26. **Requirements for financial institutions and designated non-financial businesses and professions** - The FATF Recommendations state that financial institutions or designated non-financial businesses and professions "should" or "should be required by law or regulation to" take certain actions. These references require countries or their competent authorities to take measures that will oblige their financial institutions or designated non-financial businesses and professions to comply with each of the relevant Recommendations. In the Methodology, in order to use one consistent phrase, the criteria relevant to financial institutions use the phrase "Financial institutions should be required" (a similar approach is taken for designated non-financial businesses).

27. **Law or regulation or other enforceable means** - The Interpretative Notes also require that "The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation". *Law or regulation* refers to primary and secondary legislation, such as laws, decrees, implementing regulations or other similar requirements, issued or authorised by a legislative body, and which impose mandatory requirements with sanctions for non-compliance. *Other enforceable means* refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority) or an SRO*. In both cases, the sanctions for non-compliance should be effective, proportionate and dissuasive (see R.17). The Methodology criteria in respect of Recommendations 5, 10 and 13 that are basic obligations are marked with an asterisk (*). More detailed elements in the criteria in respect of Recommendations 5, 10 and 13, as well as obligations under Recommendations 6-9, 11, 14-15, 18, and 21-22 could be required either by law or regulation or by other enforceable means.

28. **Assessment for designated non-financial businesses and professions** - Under Recommendations 12 and 16 designated non-financial businesses and professions should be required to take certain actions. Assessors should assess compliance on the basis that all the designated categories of non-financial businesses and professions should meet the requirements set out in the Recommendation. However, it is not necessary to require these actions through laws, regulations or other enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws, regulations or other enforceable means covering the underlying activities. Assessors should note that compliance by designated non-financial businesses and professions with all the necessary AML/CFT measures is to be assessed only under Recommendations 12 & 16, and not under other Recommendations. Failure by a country to extend the AML/CFT obligations to such businesses and professions should not be reflected in the assessment of the other Recommendations. In determining whether laws, regulations or other enforceable means should be used for particular criteria, assessors should take a corresponding approach to that used for financial institutions.

*Note to assessors: assessors should consider all the following factors when determining whether a document or mechanism has requirements that amount to "other enforceable means":

1. There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations – does the language used in the document set out or underpin clearly stated requirements which are understood as such.

(Examples:

- if particular measures use the word "shall" or "must" this should be considered mandatory;

- if they use "should" this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures "are encouraged", "are recommended" or institutions "should consider" is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory unless the country can demonstrate otherwise).

2. The document/mechanism must be issued by a competent authority (this could be a financial supervisory authority or another competent authority) or an SRO using powers delegated by such an authority or provided directly by law.

3. There must be sanctions for non-compliance (sanctions need not be in the same document that imposes the requirement, and can be in another document provided there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive – this involves consideration of the following issues:

(i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;
(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements such as not having proper systems and controls or not operating in a safe and sound manner is satisfactory provided that at a minimum, (a) the broader requirement is clearly laid out in law or regulation, (b) financial institutions could be (and have been as appropriate) adequately sanctioned for failing to comply with the requirement, and (c) a failure to meet one or more AML/CFT requirements could of itself result in a finding that the institution had failed to meet the broader requirement in appropriate cases e.g. there should not be a need to show additional prudential or other failings unrelated to AML/CFT; and
(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.
(iv) depending on the nature of the legal system, whether sanctions applied for non-compliance with requirements in an OEM document or mechanism can be appealed to a court or other body may be an element that indicates the importance of the requirements.

In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

THE FORTY RECOMMENDATIONS
Essential Criteria and Additional Elements

A. LEGAL SYSTEMS

Scope of the Criminal Offence of Money Laundering

Recommendation 1

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 1 and Special Recommendation II. (Note to assessors: Ensure that the assessments of Criteria 1.3 – 1.6 and Criteria II.2 – II.3 (in SR.II) are consistent.)

Essential criteria

1.1 Money laundering should be criminalised on the basis of the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Pyschotropic Substances (the Vienna Convention) and the 2000 UN Convention against Transnational Organized Crime (the Palermo Convention) i.e. the physical and material elements of the offence (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention).

1.2 The offence of ML should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime.

1.2.1 When proving that property is the proceeds of crime it should not be necessary that a person be convicted of a predicate offence[2].

1.3 The predicate offences for money laundering should cover all serious offences, and countries should seek to extend this to the widest range of predicate offences. At a minimum, predicate offences should include a range of offences in each of the designated categories of offences[3]. Where the designated category is limited to a specific offence, then that offence must be covered.

1.4 Where countries apply a threshold approach or a combined approach that includes a threshold approach[4], predicate offences should at a minimum comprise all offences:

a) which fall within the category of serious offences under their national law; or
b) which are punishable by a maximum penalty of more than one year's imprisonment; or
c) which are punished by a minimum penalty of more than six months imprisonment (for countries that have a minimum threshold for offences in their legal system).

---

[2] This criterion applies at any stage of the proceedings, including when a decision is being made whether to initiate proceedings.

[3] Note to assessors: R.1 does not require countries to create a separate offence of "participation in an organised criminal group and racketeering". In order to cover this category of "designated offence" (c.1.3), it is sufficient if a country meets either of the two options set out in the Palermo Convention i.e. either a separate offence or an offence based on conspiracy.

[4] Countries determine the underlying predicate offences for money laundering by reference to (a) all offences, or (b) to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or (c) to a list of predicate offences, or (d) a combination of these approaches.

Examples of categories of serious offences include: "indictable offences" (as opposed to summary offences), "felonies" (as opposed to misdemeanours); "crimes" (as opposed to délits).

1.5 Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically.

1.6 The offence of money laundering should apply to persons who commit the predicate offence. However, countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

1.7 There should be appropriate ancillary offences to the offence of money laundering, including association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law[5].

Additional elements

1.8 Where the proceeds of crime are derived from conduct that occurred in another country, which is not an offence in that other country but which would have constituted a predicate offence had it occurred domestically, does this constitute a money laundering offence?

Recommendation 2

The essential criteria listed below should be read in conjunction with the text of Recommendation 2.

Essential criteria

2.1 The offence of ML should apply at least to natural persons that knowingly engage in ML activity.

2.2 The law should permit the intentional element of the offence of ML to be inferred from objective factual circumstances.

2.3 Criminal liability for ML should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.

2.4 Making legal persons subject to criminal liability for ML should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

2.5 Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for ML. [6]

---

[5] In assessing ancillary offences to money laundering and terrorist financing, assessors should consider the substance of the available offences and not just the form. They should make sure that there are measures in national law to cover the widest possible range of ancillary offences.

[6] Note to assessors: In assessing whether criminal penalties are effective, proportionate and dissuasive (c.2.5) assessors should consider:

- The level of penalties (imprisonment/fines) for the offence relative to other serious offences in the assessed country;
- The level of penalties (imprisonment/fines) for ML/TF offences relative to ML/TF offences in other countries;

Provisional Measures and Confiscation

Recommendation 3

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 3 and Special Recommendation III. (Note to assessors: Ensure that the assessments of Criteria 3.1 – 3.4, Criterion 3.6 and Criterion III.11 (in SR.III) are consistent.)

Essential criteria

3.1 Laws should provide for the confiscation of property that has been laundered or which constitutes:

a) proceeds from;
b) instrumentalities used in; and
c) instrumentalities intended for use in

the commission of any ML, FT or other predicate offences, and property of corresponding value.

3.1.1 Criterion 3.1 should equally apply:

(a) to property that is derived directly or indirectly from proceeds of crime; including income, profits or other benefits from the proceeds of crime; and
(b) subject to criterion 3.5, to all the property referred to above, regardless of whether it is held or owned by a criminal defendant or by a third party.

All the property referred to in criteria 3.1 and 3.1.1 above is hereafter referred to as "property subject to confiscation".

3.2 Laws and other measures should provide for provisional measures, including the freezing and/or seizing of property, to prevent any dealing, transfer or disposal of property subject to confiscation.

3.3 Laws or measures should allow the initial application to freeze or seize property subject to confiscation to be made ex-parte or without prior notice, unless this is inconsistent with fundamental principles of domestic law.

3.4 Law enforcement agencies, the FIU or other competent authorities should be given adequate powers to identify and trace property that is, or may become subject to confiscation or is suspected of being the proceeds of crime.

3.5 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in the Palermo Convention.

3.6 There should be authority to take steps to prevent or void actions, whether contractual or otherwise, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation.

Additional elements

3.7 Do laws provide for the confiscation of:

- The penalties actually imposed by the courts for ML/TF offences.

a) The property of organisations that are found to be primarily criminal in nature (i.e. organisations whose principal function is to perform or assist in the performance of illegal activities)?
b) Property subject to confiscation, but without a conviction of any person (*civil forfeiture*), in addition to the system of confiscation triggered by a criminal conviction?
c) Property subject to confiscation, and which require an offender to demonstrate the lawful origin of the property?

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Recommendation 4

The essential criteria listed below should be read in conjunction with the text of Recommendation 4.

Essential criteria

4.1 Countries should ensure that no financial institution secrecy law will inhibit the implementation of the FATF Recommendations. Areas where this may be of particular concern are the ability of competent authorities to access information they require to properly perform their functions in combating ML or FT; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions where this is required by R.7, R.9 or SR.VII.

Customer Due Diligence and Record-keeping

Recommendation 5

The essential criteria listed below should be read in conjunction with the text of Recommendations 5 and 8, Special Recommendation VII, the Interpretative Notes to Recommendation 5, 12 and 16, and to Recommendation 5. (Note to assessors: Ensure that the assessments of Criteria 5.2 – 5.3 and Criterion VII.1 (in SR.VII) are consistent.)

Essential criteria

5.1* Financial institutions should not be permitted to keep anonymous accounts or accounts in fictitious names.

Where numbered accounts exist, financial institutions should be required to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. For example, the financial institution should properly identify the customer in accordance with these criteria, and the customer identification records should be available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

When CDD is required[7]

5.2* Financial institutions should be required to undertake customer due diligence (CDD) measures when:

a) establishing business relations;
b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000). This also includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
c) carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;
d) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

[7] Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction.

e) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Required CDD measures[8]

5.3* Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal persons or legal arrangements) and verify that customer's identity using reliable, independent source documents, data or information (identification data)[9].

5.4 For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a)* verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; and
(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

5.5* Financial institutions should be required to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner[10] using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.

5.5.1* For all customers, the financial institution should determine whether the customer is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

5.5.2 For customers that are legal persons or legal arrangements, the financial institution should be required to take reasonable measures to:

(a) understand the ownership and control structure of the customer;
(b)* determine who are the natural persons that ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Examples of the types of measures that would be normally needed to satisfactorily perform this function include:

- For companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company.
- For trusts - identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries.

[8] The general rule is that customers should be subject to the full range of CDD measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the CDD measures on a risk sensitive basis.

[9] Examples of the types of customer information that could be obtained, and the identification data that could be used to verify that information is set out in the paper entitled General Guide to Account Opening and Customer Identification issued by the Basel Committee's Working Group on Cross Border Banking.

[10] For life and other investment linked insurance, the beneficiary under the policy must also be identified and verified. See criteria 5.14 concerning the timing of such measures.

Note to assessors: where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the shareholders of that public company.

5.6 Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.

5.7* Financial institutions should be required to conduct ongoing due diligence on the business relationship.

5.7.1 Ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

5.7.2 Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

Risk

5.8 Financial institutions should be required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.

Examples of higher risk categories (which are derived from the Basel CDD Paper) may include[11]

a) Non-resident customers,
b) Private banking,
c) Legal persons or arrangements such as trusts that are personal assets holding vehicles,
d) Companies that have nominee shareholders or shares in bearer form.

Types of enhanced due diligence measures may include those set out in Recommendation 6.

5.9 Where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

Examples of customers, transactions or products where the risk may be lower[12] could include:

a) Financial institutions – provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are

[11] Other examples of higher risk are included in Recommendations 6 and 7.
[12] Assessors should determine in each case whether the risks are lower having regard to the type of customer, product or transaction, or the location of the customer.

supervised for compliance with those requirements.

b) Public companies that are subject to regulatory disclosure requirements. This refers to companies that are listed on a stock exchange or similar situations.

c) Government administrations or enterprises.

d) Life insurance policies where the annual premium is no more than USD/€1000 or a single premium of no more than USD/€2500.

e) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.

f) 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.

g) Beneficial owners of pooled accounts held by DNFBP provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring compliance with those requirements.

5.10 Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that the original country is satisfied are in compliance with and have effectively implemented the FATF Recommendations.

5.11 Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

5.12 Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by the competent authorities.

Timing of verification

5.13 Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

5.14 Countries may permit financial institutions to complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, provided that:

(a) This occurs as soon as reasonably practicable.
(b) This is essential not to interrupt the normal conduct of business.
(c) The money laundering risks are effectively managed.

Examples of situations where it may be essential not to interrupt the normal conduct of business are:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
- Life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, 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.

5.14.1 Where a customer is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include a set of 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 of expected norms for that type of relationship.

Failure to satisfactorily complete CDD

5.15 Where the financial institution is unable to comply with Criteria 5.3 to 5.6 above:

a) it should not be permitted to open the account, commence business relations or perform the transaction;

b) it should consider making a suspicious transaction report.

5.16 Where the financial institution has already commenced the business relationship e.g. when Criteria 5.2(e), 5.14 or 5.17 apply, and the financial institution is unable to comply with Criteria 5.3 to 5.5 above it should be required to terminate the business relationship and to consider making a suspicious transaction report.

Existing customers

5.17 Financial institutions should be required to apply CDD requirements to existing customers[13] on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

> For financial institutions engaged in banking business (and for other financial institutions where relevant) - examples of when it may otherwise be an appropriate time to do so is when: (a) a transaction of significance takes place, (b) customer documentation standards change substantially, (c) there is a material change in the way that the account is operated, (d) the institution becomes aware that it lacks sufficient information about an existing customer.

5.18 Financial institutions should be required to perform CDD measures on existing customers if they are customers to whom Criterion 5.1 applies.

Recommendation 6

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 6 and its Interpretative Note.

Essential criteria

6.1 Financial institutions should be required, in addition to performing the CDD measures required under R.5, to put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

[13] Existing customers as at the date that the national requirements are brought into force.

Examples of measures that could form part of such a risk management system include seeking relevant information from the customer, referring to publicly available information or having access to commercial electronic databases of PEPS.

6.2 Financial institutions should be required to obtain senior management approval for establishing business relationships with a PEP.

6.2.1 Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions should be required to obtain senior management approval to continue the business relationship.

6.3. Financial institutions should be required to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPS.

6.4. Where financial institutions are in a business relationship with a PEP, they should be required to conduct enhanced ongoing monitoring on that relationship.

Additional elements

6.5 Are the requirements of R.6 extended to PEPS who hold prominent public functions domestically?

6.6 Has the 2003 United Nations Convention against Corruption been signed, ratified, and fully implemented?

Recommendation 7

The essential criteria listed below should be read in conjunction with the text of Recommendation 7.

Essential criteria

In relation to cross-border correspondent banking and other similar relationships[14] financial institutions should, in addition to performing any CDD measures that may be required under R.5, be required to take the measures set out in Criteria 7.1-7.5.

7.1 Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

7.2 Assess the respondent institution's AML/CFT controls, and ascertain that they are adequate and effective.

7.3 Obtain approval from senior management before establishing new correspondent relationships.

7.4 Document[15] the respective AML/CFT responsibilities of each institution.

[14]Similar relationships to which financial institutions should apply Criteria 7.1-7.5 include for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

[15]It is not necessary that the two financial institutions always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures.

7.5 Where a correspondent relationship involves the maintenance of "payable-through accounts", financial institutions should be satisfied that:

(a) their customer (the respondent financial institution) has performed all the normal CDD obligations set out in R.5 on those of its customers that have direct access to the accounts of the correspondent financial institution; and
(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

Recommendation 8

The essential criteria listed below should be read in conjunction with the text of Recommendation 8.

Essential criteria

8.1 Financial institutions should be required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

8.2 Financial institutions should be required to have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures should apply when establishing customer relationships and when conducting ongoing due diligence.

Examples of non-face to face operations include: business relationships concluded over the Internet or by other means such as through the post; services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services; use of ATM machines; telephone banking; transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

8.2.1 Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

Examples of such procedures include: the certification of documents presented; the requisition of additional documents to complement those which are required for face-to-face customers; develop independent contact with the customer; rely on third party introduction (see criteria 9.1 to 9.5) and require the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

Financial institutions should refer to the CDD Paper, Section 2.2.6.

For electronic services, financial institutions could refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee in July 2003.

Recommendation 9

The essential criteria listed below should be read in conjunction with the text of Recommendation 9 and its Interpretative Note.

Note: This Recommendation does not apply to:

(a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution to carry out its CDD functions[16];
(b) business relationships, accounts or transactions between financial institutions for their clients. These are addressed by R.5 and R.7.

Essential criteria

If financial institutions are permitted to rely on intermediaries or other third parties to perform some of the elements of the CDD process (Criteria 5.3 to 5.6)[17] or to introduce business, then the following criteria should be met.

9.1 Financial institutions relying upon a third party should be required to immediately obtain from the third party the necessary information[18] concerning certain elements of the CDD process (Criteria 5.3 to 5.6).

9.2 Financial institutions should be required to take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.

9.3 Financial institutions should be required to satisfy themselves that the third party is regulated and supervised (in accordance with Recommendation 23, 24 and 29), and has measures in place to comply with, the CDD requirements set out in R.5 and R.10.

9.4 In determining in which countries the third party that meets the conditions can be based, competent authorities should take into account information available on whether those countries adequately apply the FATF Recommendations[19].

9.5 The ultimate responsibility for customer identification and verification should remain with the financial institution relying on the third party.

Recommendation 10

The essential criteria listed below should be read in conjunction with the text of Recommendation 10 and its Interpretative Note.

Essential criteria

10.1* Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

---

[16] Where there is a contract to outsource CDD, R.9 does not apply because the outsource or agent is to be regarded as synonymous with the financial institution i.e. the processes and documentation are those of the financial institution itself.

[17] In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another financial institution or third party. It may also occur in business relationships between insurance companies and insurance brokers/agents, or between mortgage providers and brokers.

[18] It is not necessary to obtain copies of documentation.

[19] Countries could refer to reports, assessments or reviews concerning AML/CFT that are published by the FATF, FSRBs, the IMF or World Bank.

10.1.1 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Examples of the necessary components of transaction records include: customer's (and beneficiary's) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

10.2* Financial institutions should be required to maintain records of the identification data, account files and business correspondence for at least five years following the termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

10.3* Financial institutions should be required to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

Recommendation 11

The essential criteria listed below should be read in conjunction with the text of Recommendation 11 and its Interpretative Note.

Essential criteria

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

Examples of such transactions or patterns of transactions include: significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.

11.2 Financial institutions should be required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing.

11.3 Financial institutions should be required to keep such findings available for competent authorities and auditors for at least five years.

Recommendation 12

The essential criteria listed below should be read in conjunction with the text of Recommendation 12, the Interpretative Note to R.5, 12 & 16, and the essential criteria and the additional elements for Recommendations 5, 6 and 8-11.

Essential criteria

12.1 DNFBP should be required to comply with the requirements set out in Recommendation 5 (Criteria 5.1 – 5.18) in the following circumstances[20]:

a) Casinos (including internet casinos[21]) – when their customers engage in financial transactions[22] equal to or above USD/€ 3,000[23].

[20] The designated thresholds applied in these criteria are referred to in the IN of R. 5, 12 and 16.

Examples of financial transactions in casinos include: the purchase or cashing in of casinos chips or tokens, the opening of accounts, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that involve only casino chips or tokens.

b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate[24].

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above USD/€ 15,000.

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for a client in relation to the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets[25];
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and Company Service Providers when they prepare for and when they carry out transactions for a client in relation to the following activities:

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

---

[21]Countries should establish rules to determine the basis upon which internet casinos are subject to national AML/CFT requirements. This will require the country to determine the basis or set or factors upon which it will decide whether there is a sufficient nexus or connection between the internet casino and the country. Examples of such factors include incorporation or organisation under the laws of the country, or place of effective management within the country. Assessors should examine the basis for the nexus or connection, with respect to R.12, 16 and 24.

[22]Note to assessors: Recommendation 12 (c.12.1) requires casinos (including internet casinos) to implement Recommendation 5, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/€ 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

[23]The designated thresholds of USD/€ 3,000 and USD/€ 15,000 include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

[24]This means that real estate agents should comply with R.5 with respect to both the purchasers and the vendors of the property.

[25] Where the lawyer, notary, other independent legal professional or accountant is conducting financial activity as a business and meets the definition of "financial institution" then that person or firm should comply with the requirements applicable to financial institutions.

DNFBP should especially comply with the CDD measures set out in Criteria 5.3 to 5.7 but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

12.2 In the circumstances set out in Criterion 12.1, DNFBP should be required to comply with the criteria set out under Recommendations 6 and 8-11.

Reporting of Suspicious Transactions and Compliance

Recommendation 13

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 1, Recommendation 13 and its Interpretative Note, and the text of Special Recommendation IV. (Note to assessors: Ensure that the assessments of Criteria 13.1 – 13.4 and Criteria IV.1 – IV.2 (in SR.IV) are consistent.)

Essential criteria

13.1* A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report – STR) when it suspects or has reasonable grounds to suspect[26] that funds are the proceeds of a criminal activity. At a minimum, the obligation to make a STR should apply to funds that are the proceeds of all offences that are required to be included as predicate offences under Recommendation 1. This requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a ML offence or otherwise (so called "indirect reporting"), is not acceptable.

13.2* The obligation to make a STR also applies to funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

13.3* All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

13.4 The requirement to report suspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

Additional elements

13.5 Are financial institutions required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically?

Recommendation 14

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 14 and its Interpretative Note.

[26]The requirement to report when the individual "suspects" is a subjective test of suspicion i.e. the person actually suspected that a transaction involved a criminal activity. A requirement to report when there are "reasonable grounds to suspect" is an objective test of suspicion and can be satisfied if the circumstances surrounding the transaction would lead a reasonable person to suspect that the transaction involved a criminal activity. This requirement implies that countries may choose either the two alternatives, but need not have both.

Essential criteria

14.1. Financial institutions and their directors, officers and employees (permanent and temporary) should be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. This protection should be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

14.2. Financial institutions and their directors, officers and employees (permanent and temporary) should be prohibited by law from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU.

Additional elements

14.3 Do laws or regulations or any other measures ensure that the names and personal details of staff of financial institutions that make a STR are kept confidential by the FIU?

Recommendation 15

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 15 and its Interpretative Note.

Essential criteria

The type and extent of measures to be taken for each of the requirements set out below should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

15.1 Financial institutions should be required to establish and maintain internal procedures, policies and controls to prevent ML and FT, and to communicate these to their employees. These procedures, policies and controls should cover, *inter alia*, CDD, record retention, the detection of unusual and suspicious transactions and the reporting obligation.

15.1.1 Financial institutions should be required to develop appropriate compliance management arrangements e.g. for financial institutions at a minimum the designation of an AML/CFT compliance officer at the management level.

15.1.2 The AML/CFT compliance officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records, and other relevant information.

15.2 Financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with these procedures, policies and controls.

15.3 Financial institutions should be required to establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting.

15.4. Financial institutions should be required to put in place screening procedures to ensure high standards when hiring employees.

Additional elements

15.5 Is the AML/CFT compliance officer able to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors?

Recommendation 16

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 16 and its Interpretative Note, Recommendations 13-15 and their Interpretative Notes and their essential criteria / additional elements, and Special Recommendation IV.

Essential criteria

16.1 DNFBP should be required to comply with the requirements set out in Recommendation 13 (Criteria 13.1 – 13.4)[27] in the following circumstances:

a) Casinos (which includes internet casinos) and real estate agents – in the circumstances set out in R.13.
b) Dealers in precious metals or stones - when they engage in any cash transaction equal to or above USD/€ 15,000[28].
c) Lawyers, notaries, other independent legal professionals and accountants - when, on behalf of or for a client, they engage in a financial transaction in relation to the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

Note on legal professional privilege or legal professional secrecy.

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to legal professional privilege or legal professional secrecy.

It is for each jurisdiction to determine the matters that would fall under legal professional privilege or legal professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

[27] DNFBP should comply with all the criteria in Recommendation 13 with two exceptions. First, dealers in precious metals and stones must comply with criteria 13.3, but would only be required to report transactions (or attempted transactions) above the cash threshold of USD/€ 15,000. Second, as detailed in criteria 16.1, countries may allow lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals to send their STR to self-regulatory organizations, and they do not always need to send STR to the FIU.

[28] The designated threshold includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked (cases of "smurfing"/"structuring").

d) Trust and Company Service Providers - when they prepare for or carry out a transaction on behalf of a client, in relation to the following activities:

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

16.2 Where countries allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations (SRO), there should be appropriate forms of co-operation between these organisations and the FIU. Each country should determine the details of how the SRO could co-operate with the FIU.

16.3 In the circumstances set out in criterion 16.1, the criteria set out under Recommendations 14, 15 and 21 should apply in relation to DNFBP.

Additional elements

16.4 Is the reporting requirement extended to the rest of the professional activities of accountants, including auditing?

16.5 Are DNFBP required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically?

Other Measures to Deter Money Laundering and Terrorist Financing

Recommendation 17

The essential criteria listed below should be read in conjunction with the text of Recommendation 17, Special Recommendations IV, VI and VII. (Note to assessors: Ensure that Criteria 17.1 – 17.4 and Criterion VI.5 (in SR.VI) and Criterion VII.9 (in SR.VII) are consistent.)

Essential criteria

17.1 Countries should ensure that effective, proportionate and dissuasive criminal, civil or administrative sanctions are available to deal with natural or legal persons covered by the FATF Recommendations that fail to comply with national AML/CFT requirements.

17.2 Countries should designate an authority (e.g. supervisors or the FIU) empowered to apply these sanctions. Different authorities may be responsible for applying sanctions depending on the nature of the requirement that was not complied with.

17.3 Sanctions should be available in relation not only to the legal persons that are financial institutions or businesses but also to their directors and senior management.

17.4 The range of sanctions available should be broad and proportionate to the severity of a situation. They should include the power to impose disciplinary and financial sanctions and the power to withdraw, restrict or suspend the financial institution's license, where applicable.

> Examples of types of sanctions include: written warnings (separate letter or within an audit report), orders to comply with specific instructions (possibly accompanied with daily fines for non-compliance), ordering regular reports from the institution on the measures it is taking, fines for non compliance, barring individuals from employment within that sector, replacing or restricting the powers of managers, directors, or controlling owners, imposing conservatorship or a suspension or withdrawal of the license, or criminal penalties where permitted.

Recommendation 18

The essential criteria listed below should be read in conjunction with the text of Recommendation 18.

Essential criteria

18.1 Countries should not approve the establishment or accept the continued operation of shell banks.

18.2 Financial institutions should not be permitted to enter into, or continue, correspondent banking relationships with shell banks.

18.3 Financial institutions should be required to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

Recommendation 19

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 19.

Essential criteria

19.1 Countries should consider the feasibility and utility of implementing a system where financial institutions report all transactions in currency above a fixed threshold to a national central agency with a computerised data base.

Additional elements

19.2 Where systems for reporting large currency transactions are in place, are the reports maintained in a computerised data base, available to competent authorities for AML/CFT purposes?

19.3 Are the systems for reporting large currency transactions subject to strict safeguards to ensure proper use of the information or data that is reported or recorded?

Recommendation 20

The essential criteria listed below should be read in conjunction with the text of Recommendation 20.

Essential criteria

20.1 Countries should consider applying Recommendations 5, 6, 8-11, 13-15, 17 and 21 to non-financial businesses and professions (other than DNFBP) that are at risk of being misused for money laundering or terrorist financing.

Examples of businesses or professions that may be at risk include: dealers in high value and luxury goods, pawnshops, gambling, auction houses and investment advisers.

20.2 Countries should take measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering.

Examples of techniques or measures that may be less vulnerable to money laundering include:

- Reducing reliance on cash;
- Not issuing very large denomination banknotes;
- Secured automated transfer systems.

Recommendation 21

The essential criteria listed below should be read in conjunction with the text of Recommendation 21.

Essential criteria

21.1 Financial institutions should be required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations.

21.1.1 There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

21.2 If those transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors.

21.3 Where a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate counter-measures.

Examples of possible counter-measures 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 countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;
- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering.
- Limiting business relationships or financial transactions with the identified country or persons in that country.

Recommendation 22

The essential criteria listed below should be read in conjunction with the text of Recommendation 22.

Essential criteria

22.1 Financial institutions should be required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e. host country) laws and regulations permit.

22.1.1 Financial institutions should be required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply the FATF Recommendations.

22.1.2 Where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries should be required to apply the higher standard, to the extent that local (i.e. host country) laws and regulations permit.

22.2 Financial institutions should be required to inform their home country supervisor when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (i.e. host country) laws, regulations or other measures.

Additional elements

22.3 Are financial institutions subject to the Core Principles required to apply consistent CDD measures at the group level, taking into account the activity of the customer with the various branches and majority owned subsidiaries worldwide?

Recommendation 23

The essential criteria listed below should be read in conjunction with the text of Recommendation 23, its Interpretative Note, the text of Special Recommendation VI, and its Interpretative Note.

Note to assessors: Assessors should use criterion 23.1 to assess the overall adequacy of the regulatory and supervisory system, and to note any deficiencies that are not dealt with in other criteria. Assessors may also wish to have regard to matters raised in assessments made with respect to the Core Principles.

Essential criteria

23.1 Countries should ensure that financial institutions are subject to adequate AML/CFT regulation and supervision and are effectively implementing the FATF Recommendations.

23.2 Countries should ensure that a designated competent authority or authorities has/have responsibility for ensuring that financial institutions adequately comply with the requirements to combat money laundering and terrorist financing.

23.3 Supervisors or other competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function, including in the executive or supervisory boards, councils, etc in a financial institution.

23.3.1 Directors and senior management of financial institutions subject to the Core Principles should be evaluated on the basis of "fit and proper" criteria including those relating to expertise and integrity.

23.4 For financial institutions that are subject to the Core Principles[29] the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes, except where specific criteria address the same issue in this Methodology.

> Examples of regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, include requirements for: (i) licensing and structure; (ii) risk management processes to identify, measure, monitor and control material risks; (iii) ongoing supervision and (iv) global consolidated supervision where required by the Core Principles.

23.5 Natural and legal persons providing a money or value transfer service, or a money or currency changing service should be licensed or registered.

23.6 Natural and legal persons providing a money or value transfer service, or a money or currency changing service should be subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

23.7 Financial institutions (other than those mentioned in Criterion 23.4) should be licensed or registered and appropriately regulated, and subject to supervision or oversight for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the required measures may be less.

Recommendation 24

The essential criteria listed below should be read in conjunction with the text of Recommendation 24.

Essential criteria

24.1 Countries should ensure that casinos (including Internet casinos) are subject to a comprehensive regulatory and supervisory regime that ensures they are effectively implementing the AML/CFT measures required under the FATF Recommendations.

24.1.1 Countries should ensure that a designated competent authority has responsibility for the AML/CFT regulatory and supervisory regime. The competent authority should have adequate powers to perform its functions, including powers to monitor and sanction (countries should ensure that criteria 17.1-17.4 apply to the obligations under R.12 and R.16).

24.1.2 Casinos should be licensed by a designated competent authority.

24.1.3 A competent authority should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino.

24.2 Countries should ensure that the other categories of DNFBP are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in that sector i.e. if there is a proven low risk then the extent of the required measures may be less.

[29] Note to assessors: refer to the Core Principles for a precise description of the financial institutions that are covered, but broadly speaking it refers to: (1) banking and other deposit-taking business, (2) insurers and insurance intermediaries, and (3) collective investment schemes and market intermediaries.

24.2.1 There should be a designated competent authority or SRO responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements. Such an authority or SRO should have:

a) Adequate powers to perform its functions, including powers to monitor and sanction (countries should ensure that criteria 17.1-17.4 apply to the obligations under R.12 and R.16).
b) Sufficient technical and other resources to perform its functions[30].

Recommendation 25

The essential criteria listed below should be read in conjunction with the text of Recommendation 25 and its Interpretative Note.

Essential criteria

25.1 Competent authorities should establish guidelines that will assist financial institutions and DNFBP to implement and comply with their respective AML/CFT requirements. For DNFBP, such guidelines may be established by SROs.

> At a minimum, the guidelines should give assistance on issues covered under the relevant FATF Recommendations, including: (i) a description of ML and FT techniques and methods; and (ii) any additional measures that these institutions and DNFBP could take to ensure that their AML/CFT measures are effective.

25.2 Competent authorities, and particularly the FIU, should provide financial institutions and DNFBP that are required to report suspicious transactions, with adequate and appropriate feedback having regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

> Examples of appropriate feedback mechanisms (drawn from the Best Practices Paper) may include:
>
> (i) general feedback - (a) statistics on the number of disclosures, with appropriate breakdowns, and on the results of the disclosures; (b) information on current techniques, methods and trends (typologies); and (c) sanitised examples of actual money laundering cases.
>
> (ii) specific or case by case feedback - (a) acknowledgement of the receipt of the report; (b) subject to domestic legal principles, if a case is closed or completed, whether because of a concluded prosecution, because the report was found to relate to a legitimate transaction or for other reasons, and if the information is available, then the institution should receive information on that decision or result.

[30] In assessing compliance with this criterion, assessors should have regard to Criteria 30.1 to 30.4 where it is appropriate to do so (i.e. depending on the type of the designated competent authority or SRO, its size, its responsibilities, etc).

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent Authorities, their Powers and Resources

Recommendation 26

The essential criteria listed below should be read in conjunction with the text of Recommendation 26 and its Interpretative Note.

Essential criteria

26.1 Countries should establish an FIU that serves as a national centre for receiving (and if permitted, requesting), analysing, and disseminating disclosures of STR and other relevant information concerning suspected ML or FT activities. The FIU can be established either as an independent governmental authority or within an existing authority or authorities.

26.2 The FIU or another competent authority should provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures that should be followed when reporting.

26.3 The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

26.4 The FIU, either directly or through another competent authority, should be authorised to obtain from reporting parties additional information needed to properly undertake its functions.

26.5 The FIU should be authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect ML or FT.

26.6 The FIU should have sufficient operational independence and autonomy to ensure that it is free from undue influence or interference.

26.7 Information held by the FIU should be securely protected and disseminated only in accordance with the law.

26.8 The FIU should publicly release periodic reports, and such reports should include statistics, typologies and trends as well as information regarding its activities.

26.9 Where a country has created an FIU, it should consider applying for membership in the Egmont Group.

26.10 Countries should have regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU).

Recommendation 27

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 27 and its Interpretative Note.

Essential criteria

27.1 There should be designated law enforcement[31] authorities that have responsibility for ensuring that ML and FT offences are properly investigated.

27.2 Countries should consider taking measures, whether legislative or otherwise, that allow competent authorities investigating ML cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering.

Additional elements

27.3 Are measures in place, whether legislative or otherwise, that provide law enforcement or prosecution authorities with an adequate legal basis for the use of a wide range of special investigative techniques when conducting investigations of ML or FT (e.g. controlled delivery of the proceeds of crime or funds intended for use in terrorism, undercover operations, etc)?

27.4 Where special investigative techniques are permitted, are such techniques used when conducting investigations of ML, FT, and underlying predicate offences, and to what extent?

27.5 In addition to special investigative techniques, are the following effective mechanisms used?

(a) Permanent or temporary groups specialised in investigating the proceeds of crime (financial investigators)? An important component of the work of such groups or bodies would be focused on the investigation, seizure, freezing and confiscation of the proceeds of crime.

(b) Co-operative investigations with appropriate competent authorities in other countries, including the use of special investigative techniques, provided that adequate safeguards are in place?

27.6 Are ML and FT methods, techniques and trends reviewed by law enforcement authorities, the FIU and other competent authorities (as appropriate) on a regular, interagency basis? Are the resulting information, analyses or studies disseminated to law enforcement and FIU staff, as well as staff of other competent authorities?

Recommendation 28

The essential criteria listed below should be read in conjunction with the text of Recommendation 28.

Essential criteria

28.1 Competent authorities responsible for conducting investigations of ML, FT and other underlying predicate offences should have the powers to be able to:

a) compel production of,
b) search persons or premises for, and
c) seize and obtain

transaction records, identification data obtained through the CDD process, account files and business correspondence, and other records, documents or information, held or maintained by financial institutions and other businesses or persons. Such powers should be exercised through lawful process (for example, subpoenas, summonses, search and seizure warrants, or court orders)

[31] In certain countries, this responsibility also rests with prosecution authorities.

and be available for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions e.g. actions to freeze and confiscate the proceeds of crime.

28.2 The competent authorities referred to above should have the powers to be able to take witnesses' statements for use in investigations and prosecutions of ML, FT, and other underlying predicate offences, or in related actions.

Recommendation 29

The essential criteria listed below should be read in conjunction with the text of Recommendation 29.

Essential criteria

29.1 Supervisors should have adequate powers to monitor and ensure compliance by financial institutions[32], with requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations.

29.2 Supervisors should have the authority to conduct inspections of financial institutions, including on-site inspections, to ensure compliance. Such inspections should include the review of policies, procedures, books and records, and should extend to sample testing.

29.3 Supervisors should have the power to compel production of or to obtain access to all records, documents or information relevant to monitoring compliance. This includes all documents or information related to accounts or other business relationships, or transactions, including any analysis the financial institution has made to detect unusual or suspicious transactions.

29.3.1 The supervisor's power to compel production of or to obtain access for supervisory purposes should not be predicated on the need to require a court order.

29.4 The supervisor should have adequate powers of enforcement and sanction against financial institutions, and their directors or senior management for failure to comply with or properly implement requirements to combat money laundering and terrorist financing, consistent with the FATF Recommendations.

Recommendation 30

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 30.

Essential criteria

30.1 FIUs, law enforcement and prosecution agencies, supervisors and other competent authorities involved in combating money laundering and terrorist financing should be adequately structured, funded, staffed, and provided with sufficient technical and other resources to fully and effectively perform their functions. Adequate structuring includes the need for sufficient operational independence and autonomy to ensure freedom from undue influence or interference.[33]

---

[32] Note to assessors: With respect to foreign branches and subsidiaries, the requirement for financial institutions to ensure that their foreign branches and subsidiaries observe AML/CFT measures is to be assessed only against R.22. However, under R.29, supervisors should have adequate powers to establish that financial institutions require their foreign branches and majority owned subsidiaries to apply R.22 effectively.

[33] If a country's FIU does not comply with the requirement to have sufficient operational independence and autonomy (Criterion 26.6), the country should only be rated down in Recommendation 26.

30.2 Staff of competent authorities should be required to maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

30.3 Staff of competent authorities should be provided with adequate and relevant training for combating ML and FT.

> Examples of issues to be covered under adequate and relevant training include: the scope of predicate offences, ML and FT typologies, techniques to investigate and prosecute these offences, techniques for tracing property that is the proceeds of crime or is to be used to finance terrorism, and ensuring that such property is seized, frozen and confiscated, and the techniques to be used by supervisors to ensure that financial institutions are complying with their obligations; the use of information technology and other resources relevant to the execution of their functions. Countries could also provide special training and/or certification for financial investigators for, *inter alia*, investigations of ML, FT, and the predicate offences.

Additional elements

30.4 Are special training or educational programmes provided for judges and courts concerning ML and FT offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism?

Recommendation 31

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 31.

Essential criteria

31.1 Policy makers, the FIU, law enforcement and supervisors and other competent authorities should have effective mechanisms in place which enable them to co-operate, and where appropriate, co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

> Such mechanisms should normally address:
>
> (a) operational co-operation and, where appropriate, co-ordination between authorities at the law enforcement/FIU level (including customs authorities where appropriate); and between the FIU, law enforcement and supervisors;
> (b) policy co-operation and, where appropriate, co-ordination across all relevant competent authorities.

Additional elements

31.2 Are mechanisms in place for consultation between competent authorities, the financial sector and other sectors (including DNFBP) that are subject to AML/CFT laws, regulations, guidelines or other measures?

Recommendation 32

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 32.

Essential criteria

32.1 Countries should review the effectiveness of their systems for combating money laundering and terrorist financing on a regular basis.

32.2 Competent authorities should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of systems for combating money laundering and terrorist financing. This should include keeping annual statistics on:

(a) suspicious transaction reports, and other reports where appropriate under domestic law, received and disseminated -

- STR received by the FIU, including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR;
- Breakdown of STR analysed and disseminated;
- Reports filed on: (i) domestic or foreign currency transactions above a certain threshold, (ii) cross border transportation of currency and bearer negotiable instruments, or (iii) international wire transfers.

(b) ML & FT investigations; prosecutions and convictions, and on property frozen; seized and confiscated -

- ML and FT investigations, prosecutions, and convictions;
- The number of cases and the amounts of property frozen, seized, and confiscated relating to (i) ML, (ii) FT, and (iii) criminal proceeds; and
- Number of persons or entities and the amounts of property frozen pursuant to or under U.N. Resolutions relating to terrorist financing.

(c) Mutual legal assistance or other international requests for co-operation -

- All mutual legal assistance and extradition requests (including requests relating to freezing, seizing and confiscation) that are made or received, relating to ML, the predicate offences and FT, including the nature of the request, whether it was granted or refused, and the time required to respond;
- Other formal requests for assistance made or received by the FIU, including whether the request was granted or refused;
- Spontaneous referrals made by the FIU to foreign authorities.

(d) Other action

- On-site examinations conducted by supervisors relating to or including AML/CFT and any sanctions applied.
- Formal requests for assistance made or received by supervisors relating to or including AML/CFT, including whether the request was granted or refused.

Additional elements

32.3 Do competent authorities maintain comprehensive statistics on:

a) STR resulting in investigation, prosecution, or convictions for ML, FT or an underlying predicate offence?

b) any criminal sanctions applied to persons convicted of ML and FT offences?

c) other formal requests for assistance made or received by law enforcement authorities relating to ML or FT, including whether the request was granted or refused?

d) the number of cases and the amounts of property frozen, seized, and confiscated relating to underlying predicate offences where applicable?

Recommendation 33

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 33.

Essential criteria

33.1 Countries should take measures to prevent the unlawful use of legal persons in relation to money laundering and terrorist financing by ensuring that their commercial, corporate and other laws require adequate transparency concerning the beneficial ownership and control of legal persons.

Examples[34] of mechanisms that countries could use in seeking to ensure that there is adequate transparency may include:

1. A system of central registration (or up front disclosure system) where a national registry records the required ownership and control details for all companies and other legal persons registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring company service providers to obtain, verify and retain records of the beneficial ownership and control of legal persons.

3. Relying on the investigative and other powers of law enforcement, regulatory, supervisory, or other competent authorities in a jurisdiction to obtain or have access to the information.

These mechanisms are, to a large degree, complementary and countries may find it highly desirable and beneficial to use a combination of them.

To the extent that countries rely on the investigative powers of their competent authorities, these authorities should have sufficiently strong compulsory powers for the purpose of obtaining the relevant information.

Whatever mechanism is used it is essential that: (a) competent authorities are able to obtain or have access in a timely fashion to the beneficial ownership and control information, (b) the information is adequate, accurate and timely (see Criterion 33.2) and (c) competent authorities are able to share such information with other competent authorities domestically or internationally.

33.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons.

[34] Note to assessors: These examples are summaries of mechanisms set out in the OECD Report "Behind the Corporate Veil. Using Corporate Entities for Illicit Purposes" 2001. An explanation of these mechanisms and their suitability is contained in the report itself.

33.3 Countries that have legal persons able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering, and that the principles set out in criteria 33.1 and 33.2 above apply equally to legal persons that use bearer shares. The measures to be taken may vary from country to country, but each country should be able to demonstrate the adequacy and effectiveness of the measures that are applied.

Additional elements

33.4 Are measures in place to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data?

Recommendation 34

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 34.

Essential criteria

34.1 Countries should take measures to prevent the unlawful use of legal arrangements in relation to money laundering and terrorist financing by ensuring that its commercial, trust and other laws require adequate transparency concerning the beneficial ownership and control of trusts and other legal arrangements.

Examples[35] of mechanisms that countries could use in seeking to ensure that there is adequate transparency may include:

1. A system of central registration (or up front disclosure system) where a national registry records details on trusts (i.e. settlors, trustees, beneficiaries and protectors) and other legal arrangements registered in that country. The relevant information could be either publicly available or only available to competent authorities. Changes in ownership and control information would need to be kept up to date.

2. Requiring trust service providers to obtain, verify and retain records of the details of the trust or other similar legal arrangements.

3. Relying on the investigative and other powers of law enforcement, regulatory, supervisory, or other competent authorities in a jurisdiction to obtain or have access to the information.

These mechanisms are, to a large degree, complementary and countries may find it highly desirable and beneficial to use a combination of them.

To the extent that countries rely on the investigative powers of their competent authorities, these authorities should have sufficiently strong compulsory powers for the purpose of obtaining the relevant information.

Whatever mechanism is used it is essential that: (a) competent authorities are able to obtain or have access in a timely fashion to the beneficial ownership and control information, (b) the information is adequate, accurate and timely (see Criterion 34.2) and (c) competent authorities are able to share such information with other competent authorities domestically or internationally.

[35] Note to assessors: These examples are summaries of mechanisms set out in the OECD Report "Behind the Corporate Veil. Using Corporate Entities for Illicit Purposes" 2001. An explanation of these mechanisms and their suitability is contained in the report itself.

34.2 Competent authorities should be able to obtain or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal arrangements, and in particular the settlor, the trustee, and the beneficiaries of express trusts.

Additional elements

34.3 Are measures in place to facilitate access by financial institutions to beneficial ownership and control information, so as to allow them to more easily verify the customer identification data?

D. INTERNATIONAL CO-OPERATION

Recommendation 35

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 35 and Special Recommendation I, and the text of the Conventions referred to in Recommendation 35[36] (Note to assessors: Ensure that the assessments of Criterion 35.1 and Criterion I.1 (in SR.I) are consistent.)

Essential criteria

35.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention).[37]

Additional elements

35.2 Have other relevant international conventions such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism been signed, ratified or fully implemented?

Recommendation 36

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 36 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 36.1 – 36.6 and Criterion V.1 (in SR.V) are consistent.)

Essential criteria

36.1 Countries should be able to provide the widest possible range of mutual legal assistance in AML/CFT investigations, prosecutions and related proceedings[38]. Mutual legal assistance should include assistance of the following nature: (a) the production, search and seizure of information, documents, or evidence (including financial records) from financial institutions, or other natural or legal persons; (b) the taking of evidence or statements from persons; (c) providing originals or copies of relevant documents and records as well as any other information and evidentiary items, (d) effecting service of judicial documents; (e) facilitating the voluntary appearance of persons for the purpose of providing information or testimony to the requesting country and (f) identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT, as well as the instrumentalities of such offences, and assets of corresponding value[39]

---

[36] Assessors should be satisfied that all the articles relevant to ML and FT are fully implemented.

[37] Assessors should be satisfied that the following relevant articles of the Vienna Convention (Articles 3-11, 15, 17 and 19), the Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31, & 34), and the Terrorist Financing Convention (Articles 2-18) are fully implemented.

[38] Note to assessors: Where the money laundering offence or the terrorist financing offence has deficiencies such as not covering all the required predicate offences, or not criminalising the financing of a terrorist organisation or individual terrorist, this may impact on the ability of the assessed country to provide international co-operation if dual criminality is a precondition for extradition or providing mutual legal assistance. This could be a factor affecting the rating.

[39] Elements (a) to (f) are drawn from the Palermo Convention.

36.1.1 Countries should be able to provide such assistance in a timely, constructive and effective manner.

36.2 Mutual legal assistance should not be prohibited or made subject to unreasonable, disproportionate or unduly restrictive conditions.

> Possible examples of such conditions (for which an assessment as to reasonableness, proportionality or restrictiveness should be made) could include: generally refusing to provide assistance on the grounds that judicial proceedings have not commenced in the requesting country; requiring a conviction before providing assistance; overly strict interpretations of the principles of reciprocity and dual criminality.

36.3 There should be clear and efficient processes for the execution of mutual legal assistance requests in a timely way and without undue delays.

36.4 A request for mutual legal assistance should not be refused on the sole ground that the offence is also considered to involve fiscal matters.

36.5 A request for mutual legal assistance should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBP, except where the relevant information was obtained in circumstances where legal professional privilege or legal professional secrecy applies[40].

36.6 The powers of competent authorities required under R.28 should also be available for use in response to requests for mutual legal assistance.

36.7 To avoid conflicts of jurisdiction, countries should consider devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Additional elements

36.8 Are the powers of competent authorities required under R.28 available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts?

Recommendation 37

The essential criteria listed below should be read in conjunction with the text of Recommendation 37 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criterion 37.1 and Criterion V.2 (in SR.V) are consistent.)

Essential criteria

37.1 To the greatest extent possible, mutual legal assistance should be rendered in the absence of dual criminality, in particular, for less intrusive and non compulsory measures.

37.2 For extradition and those forms of mutual legal assistance where dual criminality is required, the requested state (that is rendering the assistance) should have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence. Technical differences between the laws in the requesting and requested states, such as differences in the

[40] See also Criteria 16.2.

manner in which each country categorises or denominates the offence should not pose an impediment to the provision of mutual legal assistance.

Recommendation 38

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 38 and its Interpretative Note, and the text of Recommendation 3 and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 38.1 – 38.3 and Criterion 36.1 & V.3 are consistent.)

Essential criteria

38.1 There should be appropriate laws and procedures to provide an effective and timely response to mutual legal assistance requests[41] by foreign countries related to the identification, freezing, seizure, or confiscation of:

(a) laundered property from,
(b) proceeds from,
(c) instrumentalities used in, or
(d) instrumentalities intended for use in,

the commission of any ML, FT or other predicate offences.

38.2 The requirements in Criterion 38.1 should also be met where the request relates to property of corresponding value.

38.3 Countries should have arrangements for co-ordinating seizure and confiscation actions with other countries.

38.4 Countries should consider establishing an asset forfeiture fund into which all or a portion of confiscated property will be deposited and will be used for law enforcement, health, education or other appropriate purposes.

38.5 Countries should consider authorising the sharing of confiscated assets between them when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

Additional elements

38.6 Are foreign non criminal confiscation orders (as described in criterion 3.7) recognised and enforced?

Recommendation 39

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 39.

Essential criteria

39.1 Money laundering should be an extraditable offence[42]. There should be laws and procedures to extradite individuals charged with a money laundering offence.

---

[41] Note to assessors: note also R.36, footnote 37.

[42] Note to assessors: note also R.36, footnote 37.

39.2 Countries should either:

a) extradite their own nationals or,
b) where a country does not extradite its own nationals solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. In such cases, the competent authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country.

39.3 In the case referred to in criterion 39.2(b), countries should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of the prosecution.

39.4 Consistent with the principles of domestic law, countries should adopt measures or procedures that will allow extradition requests and proceedings relating to ML to be handled without undue delay.

Additional elements

39.5 Are simplified procedures of extradition in place by allowing direct transmission of extradition requests between appropriate ministries? Can persons be extradited based only on warrants of arrests or judgements? Is there a simplified procedure of extradition of consenting persons who waive formal extradition proceedings in place?

Recommendation 40

The essential criteria and additional elements listed below should be read in conjunction with the text of Recommendation 40 and its Interpretative Note, and Special Recommendation V. (Note to assessors: Ensure that the assessments of Criteria 40.1 – 40.9 and Criterion V.5 (in SR.V) are consistent.)

Essential criteria

40.1 Countries should ensure that their competent authorities are able to provide the widest range of international cooperation to their foreign counterparts.

40.1.1 Countries should be able to provide such assistance in a rapid, constructive and effective manner.

40.2 There should be clear and effective gateways, mechanisms or channels that will facilitate and allow for prompt and constructive exchanges of information directly between counterparts[43].

> Examples of gateways, mechanisms or channels used in international cooperation and exchanges of information (other than MLA or extradition) include laws allowing exchanges of information on a reciprocal basis; bilateral or multilateral agreements or arrangements such as Memorandum of Understanding (MOU); and exchanges through appropriate international or regional organisations or bodies such as Interpol or the Egmont Group of FIUs.

40.3. Such exchanges of information should be possible: (a) both spontaneously and upon request, and (b) in relation to both money laundering and the underlying predicate offences.

[43] Obstacles to a prompt and constructive exchange of information include failing to respond or take the appropriate measures in a timely way, and unreasonable delays in responding.

40.4 Countries should ensure that all their competent authorities are authorised to conduct inquiries on behalf of foreign counterparts.

40.4.1 In particular, countries should ensure that their FIU is authorised to make the following types of inquiries on behalf of foreign counterparts: (a) searching its own databases, including with respect to information related to suspicious transaction reports; (b) searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

40.5 Countries should ensure that their law enforcement authorities are authorised to conduct investigations on behalf of foreign counterparts; other competent authorities should be authorised to conduct investigations on behalf of foreign counterparts, where permitted by domestic law.

40.6 Exchanges of information should not be made subject to disproportionate or unduly restrictive conditions.

40.7 Requests for cooperation should not be refused on the sole ground that the request is also considered to involve fiscal matters.

40.8 Requests for cooperation should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBP (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies[44]).

40.9 Countries should establish controls and safeguards to ensure that information received by competent authorities is used only in an authorised manner. These controls and safeguards should be consistent with national provisions on privacy and data protection[45].

Additional elements

40.10 Are mechanisms in place to permit a prompt and constructive exchange of information with non-counterparts? Does it take place directly or indirectly[46]?

40.10.1 Does the requesting authority as a matter of practice disclose to the requested authority the purpose of the request and on whose behalf the request is made?

40.11 Can the FIU obtain from other competent authorities or other persons relevant information requested by a foreign counterpart FIU?

---

[44] See also criteria 16.2

[45] This implies that, at a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving competent authority.

[46] The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority.

NINE SPECIAL RECOMMENDATIONS
Essential Criteria and Additional Elements

Special Recommendation I

The essential criteria listed below should be read in conjunction with the text of Special Recommendation I, Recommendation 35, Special Recommendations II, III and V, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), and the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002), S/RES/1455(2003), and S/RES/1526(2004), and S/RES/1373(2001). (Note to assessors: Ensure that the assessments of Criterion I.1 and Criterion 35.1 (in R.35) are consistent. Also ensure that the assessments of SR.I, SR.II, SR.III and SR.V are consistent.)

Essential criteria

I.1 Countries should sign and ratify, or otherwise become a party to, and fully implement, the Terrorist Financing Convention[47].

I.2 Countries should fully implement the United Nations Security Council Resolutions relating to the prevention and suppression of FT. These comprise S/RES/1267(1999) and its successor resolutions and S/RES/1373(2001). This requires any necessary laws, regulations or other measures to be in place and for these provisions to cover the requirements contained in those resolutions.

Special Recommendation II

The essential criteria listed below should be read in conjunction with the text of Special Recommendation II, Special Recommendation I, Recommendations 1 and 2, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention). (Note to assessors: Ensure that the assessments of Criteria II.1 – II.3, Criterion I.1 (in SR.I) and Criteria 1.3 (in R.1) are consistent.)

Essential criteria

II.1 Terrorist financing should be criminalised consistent with Article 2 of the Terrorist Financing Convention, and should have the following characteristics:[48]

(a) Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part:

(i) to carry out a terrorist act(s);
(ii) by a terrorist organisation; or
(iii) by an individual terrorist.

(b) Terrorist financing offences should extend to any *funds* as that term is defined in the TF Convention. This includes funds whether from a legitimate or illegitimate source.

---

[47] Assessors should be satisfied that all relevant articles of the Terrorist Financing Convention are fully implemented (Articles 2-6 and 17-18 which relate to SR.II; Article 8 which relates to SR.III; and Articles 7 and 9-18 which relate to SR.V.)

[48] Note to assessors: the criminalisation of terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with SRII.

> The Terrorist Financing Convention defines *funds* as:
>
> "assets of every kind, whether tangible or intangible, movable or immovable, however, acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit."

(c) Terrorist financing offences should not require that the funds: (i) were actually used to carry out or attempt a terrorist act(s); or (ii) be linked to a specific terrorist act(s).

(d) It should also be an offence to attempt to commit the offence of terrorist financing.

(e) It should also be an offence to engage in any of the types of conduct set out in Article 2(5) of the Terrorist Financing Convention.

II.2 Terrorist financing offences should be predicate offences for money laundering.

II.3 Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur

II.4 Countries should ensure that Criteria 2.2 to 2.5 (in R.2) also apply in relation to the offence of FT[49].

Special Recommendation III

The essential criteria and additional elements listed below should be read in conjunction with the text of Special Recommendation III, its Interpretative Note, its Best Practices Paper, Special Recommendation I, Recommendation 3, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), the following United Nations Security Council Resolutions: S/RES/1267(1999), its successor resolutions 1333(2000), S/RES/1363(2001), S/RES/1390(2002), S/RES/1455(2003) and S/RES/1526(2004), S/RES/1373(2001) and S/RES/1452(2002). (Note to assessors: Ensure that the assessments of Criteria III.1 – III.12, Criteria I.1 – I.2 (in SR.I), Criterion VIII.2 (in SR.VIII) and Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) are consistent.)

Essential criteria

Freezing and, where appropriate, seizing under the relevant U.N. Resolutions:

III.1 Countries should have effective laws and procedures to freeze terrorist funds or other assets of persons designated by the United Nations Al-Qaida and Taliban Sanctions Committee in accordance with S/RES/1267(1999). Such freezing should take place without delay and without prior notice to the designated persons involved.

[49] Note to assessors: See also Recommendation 2 and footnote 5 on effective, proportionate and dissuasive criminal penalties.

S/RES/1267(1999) and its successor resolutions obligate countries to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267(1999), including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons' benefit, by their nationals or by any person within their territory. The Al-Qaida and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999) and its successor resolutions. All countries that are members of the United Nations are obligated by S/RES/1267(1999) and its successor resolutions to freeze the assets of persons and entities so designated by the Al-Qaida and Taliban Sanctions Committee.

III.2 A country should have effective laws and procedures to freeze terrorist funds or other assets of persons designated in the context of S/RES/1373(2001). Such freezing should take place without delay and without prior notice to the designated persons involved.

S/RES/1373(2001) obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective co-operation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries. When (i) a specific notification or communication is sent and (ii) the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation, the country receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

III.3 A country should have effective laws and procedures to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. Such procedures should ensure the prompt determination, according to applicable national legal principles, whether reasonable grounds or a reasonable basis exists to initiate a freezing action and the subsequent freezing of funds or other assets without delay.

III.4 The freezing actions referred to in Criteria III.1 – III.3 should extend to:

(a) funds or other assets wholly or jointly[50] owned or controlled, directly or indirectly, by designated persons, terrorists, those who finance terrorism or terrorist organisations; and

(b) funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons, terrorists, those who finance terrorism or terrorist organisations.

[50] *Jointly* refers to those assets held jointly between or among designated persons, terrorists, those who finance terrorism or terrorist organisations on the one hand, and a third party or parties on the other hand.

III.5 Countries should have effective systems for communicating actions taken under the freezing mechanisms referred to in Criteria III.1 – III.3 to the financial sector[51] immediately upon taking such action.

III.6 Countries should provide clear guidance to financial institutions and other persons or entities that may be holding targeted funds or other assets concerning their obligations in taking action under freezing mechanisms.

III.7 Countries should have effective and publicly-known procedures for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons or entities in a timely manner consistent with international obligations.

III.8 Countries should have effective and publicly-known procedures for unfreezing, in a timely manner, the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person.

III.9 Countries should have appropriate procedures for authorising access to funds or other assets that were frozen pursuant to S/RES/1267(1999) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses. These procedures should be in accordance with S/RES/1452(2002).

III.10 Countries should have appropriate procedures through which a person or entity whose funds or other assets have been frozen can challenge that measure with a view to having it reviewed by a court.

Freezing, Seizing and Confiscation in other circumstances

III.11 Countries should ensure that Criteria 3.1 – 3.4 and Criterion 3.6 (in R.3) also apply in relation to the freezing, seizing and confiscation of terrorist-related funds or other assets in contexts other than those described in Criteria III.1 – III.10.

General provisions

III.12 Laws and other measures should provide protection for the rights of bona fide third parties. Such protection should be consistent with the standards provided in Article 8 of the Terrorist Financing Convention, where applicable.

III.13 Countries should have appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing the obligations under SR III and to impose civil, administrative or criminal sanctions for failure to comply with such legislation, rules or regulations.

Additional elements

III.14 Have the measures set out in the Best Practices Paper for SR.III been implemented?

III.15 Have the procedures to authorise access to funds or other assets that were frozen pursuant to S/RES/1373(2001) and that have been determined to be necessary for basic expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses

[51] For examples of possible mechanisms to communicate actions taken or to be taken to the financial sector and/or the general public, see the FATF Best Practices paper entitled "Freezing of Terrorist Assets – International Best Practices".

been implemented? Are these procedures consistent with S/RES/1373(2001) and the spirit of S/RES/1452(2003)?

Special Recommendation IV

The essential criteria and additional elements listed below should be read in conjunction with the text of Special Recommendation IV, and Recommendations 13, 16 and 17. (Note to assessors: Ensure that the assessments of Criteria IV.1 – IV.2, Criteria 13.1 – 13.4 (in R.13), and Criteria 17.1 – 17.4 (in R.17) are consistent.)

Essential criteria

IV.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious[52] transaction report – STR) when it suspects or has reasonable grounds to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. This requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a FT offence or otherwise (so called "indirect reporting"), is not acceptable.

IV.2 Countries should ensure that Criteria 13.3 – 13.4 (in R.13) also apply in relation to the obligations under SR IV.

Special Recommendation V

The essential criteria and additional elements listed below should be read in conjunction with the text of Special Recommendation V, Special Recommendation I, Recommendations 36-40, the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention), and Special Recommendation III.

Essential criteria

V.1 Countries should ensure that Criteria 36.1 – 36.7 (in R.36) also apply to the obligations under SR.V[53].

V.2 Countries should ensure that Criteria 37.1 &37.2 (in R.37) also apply to the obligations under SR.V.

V.3 Countries should ensure that Criteria 38.1 – 38.5 (in R.38) also apply to the obligations under SR.V.

V.4 Countries should ensure that Criteria 39.1 – 39.4 (in R.39) also apply to extradition proceedings related to terrorist acts and FT.

V.5 Countries should ensure that Criteria 40.1 – 40.9 (in R.40) also apply to the obligations under SR.V.

Additional elements

V.6 Does the additional element 36.8 (in R.36) apply in relation to the obligations under SR.V?

V.7 Does additional element 38.6 (in R.38) apply in relation to the obligations under SR.V?

---

[52] Systems based on the reporting of unusual transactions (rather than suspicious transactions) are equally satisfactory.

[53] Note to assessors: note also R.36, footnote 37.

V.8 Does the additional element 39.5 (in R.39) apply extradition proceedings related to terrorist acts or FT?

V.9 Do additional elements 40.10 – 40.11 (in R.40) apply in relation to the obligations under SR.V?

Special Recommendation VI

The essential criteria and additional elements listed below should be read in conjunction with the text of Special Recommendation VI, its Interpretative Note and its Best Practices Paper, Special Recommendation VII and its Interpretative Note, and Recommendation 17. (Note to assessors: Ensure that the assessments of Criterion VI.5 and Criteria 17.1 – 17.4 (in R.17) are consistent.)

Essential criteria

VI.1 Countries should designate one or more competent authorities to register and/or licence natural and legal persons that perform money or value transfer services (MVT service operators), maintain a current list of the names and addresses of licensed and/or registered MVT service operators, and be responsible for ensuring compliance with licensing and/or registration requirements[54].

VI.2 Countries should ensure that all MVT service operators are subject to the applicable FATF Forty Recommendations (in particular Recommendations 4-11, 13-15 and 21-23) and FATF Nine Special Recommendations (in particular SR.VII)[55].

VI.3 Countries should have systems in place for monitoring MVT service operators and ensuring that they comply with the FATF Recommendations.

VI.4 Countries should require each licensed or registered MVT service operator to maintain a current list of its agents which must be made available to the designated competent authority.

VI.5 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR VI.

Additional elements

VI.6 Have the measures set out in the Best Practices Paper for SR.VI been implemented?

Special Recommendation VII

The essential criteria listed below should be read in conjunction with the text of SR.VII and its Interpretative Note, Recommendation 5 as it relates to verification of a customer's identity (see Essential Criterion 5.3) and Recommendation 17. (Note to assessors: Ensure that the assessments of Criterion VII.1, VII.9, Criterion 5.3 (in R.5) and Criteria 17.1 – 17.4 (in R.17) are consistent.)

---

[54] SR.VI does not require countries to establish a separate licensing/registration system or designate another competent authority in respect of money remitters which are already licensed/registered as financial institutions within the country, permitted to perform MVT services under the terms of their license/registration, and already subject to the full range of applicable obligations under the FATF Forty Recommendations and Nine Special Recommendations.

[55] Note to assessors: where there are deficiencies in the laws, regulations or other measures that are required to be applied to money value transfer service operators under other relevant Recommendations (such as those on customer due diligence, record keeping, reporting of suspicious transactions, or wire transfers), such deficiencies should also be noted in SR VI, and be taken into account in the assessment of the rating for SRVI.

Essential criteria

SR VII applies to cross-border and domestic transfers between financial institutions. However, SR VII is not intended to cover the following types of payments:

a. Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction, such as withdrawals from a bank account through an ATM machine, cash advances from a credit card, or payments for goods and services. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, and the necessary information should be included in the message.

b. Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

VII.1 For all wire transfers, of EUR/USD 1 000 or more, ordering financial institutions should be required to obtain and maintain [56] the following information relating to the originator of the wire transfer:

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

(This set of information is referred to as full originator information.)

For all wire transfers of EUR/USD 1 000 or more, ordering financial institutions should be required to verify the identity of the originator in accordance with Recommendation 5.

VII.2 For cross-border wire transfers of EUR/USD 1 000 or more the ordering financial institution should be required to include full originator information in the message or payment form accompanying the wire transfer.

However, if several individual cross-border wire transfers (of EUR/USD 1 000 or more) from a single originator are bundled in a batch file for transmission to beneficiaries in another country, the ordering financial institution only needs to include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country.

[56] Financial institutions do not have to repeatedly obtain originator information and verify originator identity every time a customer makes a wire transfer. Financial institutions could rely on the information already available if, as part of the customer due diligence process, they have obtained:
(i) the originator's name;
(ii) account number (or unique reference number if no account number exists); and
(iii) address (or national identity number, customer identification number, or date and place of birth if the country permits one of these pieces of information to substitute for the address)
and verified the originator's identity in accordance with Recommendation 5 (see, in particular, criterion 5.3). This does not apply to occasional customers.

VII.3 For domestic wire transfers the ordering financial institution should be required to either: (a) comply with Criterion VII.2 above or (b) include only the originator's account number or a unique identifier, within the message or payment form. The second option should be permitted only if full originator information can be made available to the beneficiary financial institution and to appropriate authorities within three business days of receiving a request, and domestic law enforcement authorities can compel immediate production of it.

> Note to assessors: domestic transfer (see definition in the Glossary) also refers to any chain of wire transfers that takes place entirely within the borders of the European Union. Having regard to the fact that: (1) the European Union constitutes an autonomous entity with its own sovereign rights and a legal order independent of the Member States, to which both the Member States themselves and their nationals are subject, within the European Union's areas of competence; (2) the European Union has enacted legislation binding upon its Member States, subject to control by a court of justice, which provides for the integration of payment services within an internal market in accordance with the principles of the free movement of capital and free provision of services; and (3) this legislation notably provides for the implementation of Special Recommendation VII as a single jurisdiction and requires that full information on the payer is made readily available, where appropriate upon request, to the beneficiary financial institution and relevant competent authorities.
>
> It is further noted that the European internal market and corresponding legal framework is extended to the members of the European Economic Area.

VII.4 Each intermediary and beneficiary financial institution in the payment chain should be required to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer.

VII.4.1. Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

VII.5 Beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SR.VII standards.

VII.6 Countries should have measures in place to effectively monitor the compliance of financial institutions with rules and regulations implementing SR.VII.

VII.7 Countries should ensure that Criteria 17.1 – 17.4 (in R.17) also apply in relation to the obligations under SR.VII.

Additional elements

VII.8 Countries may require that all incoming cross-border wire transfers (including those below EUR/USD 1 000) contain full and accurate originator information.

VII.9 Countries may require that all outgoing cross-border wire transfers below EUR/USD 1 000 contain full and accurate originator information.

Special Recommendation VIII

The essential criteria and additional elements listed below should be read in conjunction with the text of Special Recommendation VIII, its Interpretative Note and its Best Practices Paper.

Essential criteria

Reviews of the domestic non-profit sector:

VIII.1 Countries should: (i) review the adequacy of domestic laws and regulations that relate to non-profit organisations; (ii) use all available sources of information to undertake domestic reviews of or have the capacity to obtain timely information on the activities, size and other relevant features of their non-profit sectors for the purpose of identifying the features and types of non-profit organisations (NPOs) that are at risk of being misused for terrorist financing by virtue of their activities or characteristics; and (iii) conduct periodic reassessments by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

Some examples of possible sources of information that could be used to undertake a domestic review or provide timely information on the activities, size and other relevant features of the domestic non-profit sector are: regulators, statistical institutions, tax authorities, FIUs, donor organisations, self-regulatory organizations or accreditation institutions, or law enforcement and intelligence authorities.

Protecting the NPO sector from terrorist financing through outreach and effective oversight:

VIII.2 Countries should undertake outreach to the NPO sector with a view to protecting the sector from terrorist financing abuse. This outreach should include (i) raising awareness in the NPO sector about the risks of terrorist abuse and the available measures to protect against such abuse; and (ii) promoting transparency, accountability, integrity, and public confidence in the administration and management of all NPOs.

An effective outreach program with the NPO sector may include the development of best practices to address terrorist financing risks, regular outreach events with the sector to discuss scope and methods of abuse of NPOs, emerging trends in terrorist financing and new protective measures, and the issuance of advisory papers and other useful resources.

VIII.3 Countries should be able to demonstrate that the following steps have been taken to promote effective supervision or monitoring of those NPOs which account for: (i) a significant portion of the financial resources under control of the sector; and (ii) a substantial share of the sector's international activities.

VIII.3.1 NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through appropriate authorities.

VIII.3.2 Countries should be able to demonstrate that there are appropriate measures in place to sanction violations of oversight measures or rules by NPOs or persons acting on behalf of NPOs.

The application of such sanctions should not preclude parallel civil, administrative, or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

Sanctions may include freezing of accounts, removal of trustees, fines, de-certification, de-licensing or de-registration.

VIII.3.3 NPOs should be licensed or registered. This information should be available to competent authorities.[57]

VIII.3.4 NPOs should maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation. This also applies to information mentioned in paragraphs (i) and (ii) of the Interpretative Note to Special Recommendation VIII.

Targeting and attacking terrorist abuse of NPOs through effective information gathering, investigation:

VIII.4 Countries should implement measures to ensure that they can effectively investigate and gather information on NPOs.

VIII.4.1 Countries should ensure effective domestic co-operation, co-ordination and information sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs of potential terrorist financing concern.

VIII.4.2 Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

VIII.4.3 Countries should develop and implement mechanisms for the prompt sharing of information among all relevant competent authorities in order to take preventative or investigative action when there is suspicion or reasonable grounds to suspect that a particular NPO is being exploited for terrorist financing purposes or is a front organization for terrorist fundraising. Countries should have investigative expertise and capability to examine those NPOs that are suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations. Countries should also have mechanisms in place that allow for prompt investigative or preventative action against such NPOs.

Responding to international requests for information about an NPO of concern:

VIII.5 Countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs that are suspected of terrorist financing or other forms of terrorist support.

[57] Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

Special Recommendation IX

The essential criteria listed below should be read in conjunction with the text of Special Recommendation IX and its Interpretative Note.

Essential criteria

For a supra-national approach to Special Recommendation IX, the supra-national jurisdiction will require a supra-national assessment to determine jurisdictional compliance and all member jurisdictions should adhere to modified essential criteria (as annotated in italics below). An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of its SRIX compliance. Under this approach, the following changes shall also apply to the essential criteria:

- *Country* shall refer to the supra-national jurisdiction.
- *Cross-border* shall refer to movements that cross the external borders of the supra-national jurisdiction.
- *Domestic* shall refer to matters under the auspices of the supra-national jurisdiction, to include all relevant authorities from all individual member states which comprise a supra-national jurisdiction.
- *International* shall refer to matters outside the auspices of the supra-national jurisdiction.
- *Supra-national jurisdiction* shall refer to an autonomous entity with its own sovereign rights and legal order independent of its member states, to which both its member states and their nationals and residents are subject, and which includes binding and enforceable legislation on all member states regarding the obligatory declaration or disclosure of physical cross-border transportation of currency or bearer negotiable instruments, without prejudice to national legislation.

IX.1 To detect the physical cross-border transportation of currency and bearer negotiable instruments that are related to money laundering or terrorist financing, a country should implement one of the following two systems for incoming and outgoing[58] cross-border transportations of currency or bearer negotiable instruments[59]:

(a) A declaration system that has the following characteristics:

(i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments that are of a value exceeding a prescribed threshold should be required to submit a truthful declaration to the designated competent authorities; and

(ii) The prescribed threshold cannot exceed EUR/USD 15,000[60]

OR

(b) A disclosure system that has the following characteristics:

[58] Countries can use one or both systems for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments.

[59] Countries should implement Special Recommendation IX without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.

[60] Countries that implement a declaration system should ensure that the prescribed threshold is sufficiently low to meet the objectives of Special Recommendation IX. In any event, the threshold cannot exceed EUR/USD 15,000.

(i) All persons making a physical cross-border transportation of currency or bearer negotiable instruments should be required to make a truthful disclosure to the designated competent authorities upon request; and

(ii) The designated competent authorities should have the authority to make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

IX.2 Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.

IX.3 The designated competent authorities should be able to stop or restrain currency or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found:

(a) Where there is a suspicion of money laundering or terrorist financing; or

(b) Where there is a false declaration/disclosure.

IX.4 At a minimum, information on the amount of currency or bearer negotiable instruments declared/disclosed or otherwise detected, and the identification data of the bearer(s) shall be retained for use by the appropriate authorities in instances when:

(a) A declaration which exceeds the prescribed threshold is made; or

(b) Where there is a false declaration/disclosure; or

(c) Where there is a suspicion of money laundering or terrorist financing.

For a supra-national approach: The term *appropriate authorities* must include designated competent authorities for every member state.

IX.5 Information obtained through the processes implemented in Criterion IX.1 should be available to the financial intelligence unit (FIU) either through:

(a) A system whereby the FIU is notified about suspicious cross-border transportation incidents; or

(b) By making the declaration/disclosure information directly available to the FIU in some other way.

For a supra-national approach, the information collected through the processes described under a) or b) should be made available to the FIUs of other member states.

IX.6 At the domestic level, there should be adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Special Recommendation IX.

IX.7 At the international level, countries should allow for the greatest possible measure of co-operation and assistance amongst competent authorities, consistent with the obligations under Recommendations 35 to 40 and Special Recommendation V.

Examples of possible measures (drawn from the Best Practices Paper to Special Recommendation IX) include:

- Having co-operation arrangements with other countries which would allow for bilateral customs-to-customs information exchanges between customs and other relevant agencies on cross-border transportation reports and cash seizures.
- Ensuring that the information recorded pursuant to criterion IX.4 can be shared internationally with foreign competent authorities in appropriate cases.

For a supra-national approach: Regarding co-operation and assistance at the international level, member states' authorities should endeavour to identify the relevant sources of the information requested by third countries' authorities, when it is not possible for the member states' authorities to make this information directly available.

IX.8 Countries should ensure that Criteria 17.1 to 17.4 (in R.17) also apply to persons who make a false declaration or disclosure contrary to the obligations under SR IX.

IX.9 Countries should ensure that Criteria 17.1 to 17.4 (in R.17) also apply to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering contrary to the obligations under SR IX.

IX.10 Countries should ensure that Criteria 3.1 to 3.6 (in R.3) also apply in relation to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

IX.11 Countries should ensure that Criteria III.1 to III.10 (in SR.III) also apply in relation to persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing.

IX.12 If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should co-operate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.

IX.13 The systems for reporting cross border transactions should be subject to strict safeguards to ensure proper use of the information or data that is reported or recorded. For a supra-national approach: Any safeguards implemented for this purpose should not impede information sharing within the supra-national jurisdiction.

IX. 14 Training, data collection, enforcement (including R.17) and targeting programmes should be developed and applied by all jurisdictions. For a supra-national approach, there should be comparable: (1) training, (2) data collection, (3) enforcement (including R.17) and (4) targeting programmes developed and applied across all member states in order to ensure the equivalent application of this standard.

IX.15 For a supra-national approach, member states should ensure that all relevant authorities from each member state have access on a timely basis to all supra-national information obtained through the process implemented in Criterion IX.1. Member states should at a minimum ensure that all relevant authorities from each member state have access immediately to all supra-national information related to suspicious cash declarations/disclosures (false or not) or intentional lack of declaration/disclosure. All other supra-national information obtained through the process implemented in Criterion IX.1 should be accessible upon request.

Additional elements

IX. 16 Has the country implemented or considered implementing the measures set out in the Best Practices Paper for SR.IX?

IX.17 Where systems for reporting the cross border transportation of currency are in place, are the reports maintained in a computerised data base, available to competent authorities for AML/CFT purposes?

Annex 1:
GLOSSARY OF DEFINITIONS USED IN THE METHODOLOGY

Terms	Definition
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Agent	For the purposes of Special Recommendation VI, an *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.)
Appropriate authorities	The term *appropriate authorities* refers to competent authorities, self-regulatory bodies, accrediting institutions and other administrative authorities.
Associate NPOs	The term *associate NPOs* includes foreign branches of international NPOs
Batch transfer	A *batch transfer* is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Bearer negotiable instruments	*Bearer negotiable instruments* includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiary	For the purposes of Special Recommendation VIII, the term *beneficiaries* refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO. For the purposes of the other FATF Recommendations, the term *beneficiary* is as follows. All trusts (other than charitable or statutory permitted non-charitable trusts) must have *beneficiaries*, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.

Terms	Definition
Competent authorities	*Competent authorities* refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.
Confiscation	The term *confiscation*, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. (Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.)
Consider	References in the Recommendations that require a country to *consider* taking particular measures means that the country should have made a proper consideration or assessment of whether to implement such measures.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations and in this Methodology to *country* or *countries* apply equally to territories or jurisdictions[61].
Cross-border transfer	*Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.
Currency	Currency refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: • participation in an organised criminal group and racketeering; • terrorism, including terrorist financing; • trafficking in human beings and migrant smuggling;

[61] See also the "Note to assessors" under C.VII.3 of the Methodology.

Terms	Definition
	• sexual exploitation, including sexual exploitation of children; • illicit trafficking in narcotic drugs and psychotropic substances; • illicit arms trafficking; • illicit trafficking in stolen and other goods; • corruption and bribery; • fraud; • counterfeiting currency; • counterfeiting and piracy of products; • environmental crime; • murder, grievous bodily injury; • kidnapping, illegal restraint and hostage-taking; • robbery or theft; • smuggling; • extortion; • forgery; • piracy; and • insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

Terms	Definition
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos (which also includes internet casinos). b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: • acting as a formation agent of legal persons; • acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; • providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; • acting as (or arranging for another person to act as) a trustee of an express trust; • acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person	The term *designated persons* refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).
Designated threshold	*Designated threshold* refers to the amount set out in the Interpretative Notes to the Forty Recommendations.

Terms	Definition
Domestic transfer	*Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction[62].
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	*False declaration* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	*False disclosure* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
FATF Recommendations	*The FATF Recommendations* refers to the Forty Recommendations and to the Nine Special Recommendations on Terrorist Financing.
Financial institutions	*Financial institutions*[63] means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[64] 2. Lending.[65] 3. Financial leasing.[66] 4. The transfer of money or value.[67] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).

[62] See also the "Note to assessors" under C.VII.3 of the Methodology.
[63] For the purposes of Special Recommendation VII, it is important to note that the term *financial institution* does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.
[64] This also captures private banking.
[65] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).
[66] This does not extend to financial leasing arrangements in relation to consumer products.
[67] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

Terms	Definition
	6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[68]. 13. Money and currency changing. When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially. In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.
FIU	FIU means financial intelligence unit.
Foreign counterparts	This refers to the authorities in another country that exercise similar responsibilities and functions.
Freeze	This means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level

[68] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definition
	of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	Except in the case of Special Recommendation II, *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.
Funds transfer	The terms *funds transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
Identification data	Reliable, independent source documents, data or information will be referred to as "identification data".
Intermediaries	*Intermediaries* can be financial institutions, DNFBP or other reliable persons or businesses that meet Criteria 9.1 to 9.4.
Investigations, prosecutions and related proceedings	*Investigations, prosecutions and related proceedings* may be of a criminal, civil enforcement or administrative nature, and includes proceedings in relation to confiscation or provisional measures.
Law or regulation	*Law or regulation* refers to primary and secondary legislation, such as laws, decrees, implementing regulations or other similar requirements, issued or authorised by a legislative body, and which impose mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.
Licensing	For the purposes of Special Recommendation VI only, *licensing* means a requirement to obtain permission from a designated competent authority in order to

Terms	Definition
	operate a money/value transfer service legally.
Money laundering (ML) offence	References in this Methodology (except in R.1) to a *money laundering (ML) offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer service* refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment. A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (*or *parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala*, *hundi*, *fei-chien*, and the *black market peso exchange*. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.)
Non-profit organisations	The term *non-profit organisation* or *NPO* refers to a legal entity or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
Originator	The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.
Other enforceable means	Other enforceable means refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority) or an SRO. The sanctions for non-compliance should be effective, proportionate and dissuasive.
Palermo Convention	The 2000 UN Convention against Transnational Organized Crime.
Payable-through accounts	*Payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Physical cross-border transportation	*Physical cross-border transportation* refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency through containerised cargo or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

Terms	Definition
Politically Exposed Persons" (PEPs)	*PEPs* are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Registration	For the purposes of Special Recommendation VI, *registration* means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.
Related to terrorist financing or money laundering	When used to describe currency or bearer negotiable instruments, the term *Related to terrorist financing or money laundering* refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.
Risk	All references to *risk* in this Methodology refer to the risk of money laundering and/or terrorist financing.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.
Self-regulatory organisation (SRO)	A *SRO* is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Terms	Definition
Settlor	*Settlors* are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
S/RES/1267(1999)	The term *S/RES/1267(1999)* refers to S/RES/1267(1999) and its successor resolutions. When issued, S/RES/1267(1999) had a time limit of one year. A series of resolutions have been issued by the United Nations Security Council (UNSC) to extend and further refine provisions of S/RES/1267(1999). By successor resolutions are meant those resolutions that extend and are directly related to the original resolution S/RES/1267(1999). As of February 2004, these resolutions included S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002), S/RES/1455(2003) and S/RES/1526(2004).
STR	*STR* refers to suspicious transaction reports.
Subsidiaries	*Subsidiaries* refers to majority owned subsidiaries.
Supervisors	*Supervisors* refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.
Terrorist	For purposes of SRIII, the term *terrorist* is as defined in the Interpretative Note of SRIII. Otherwise, it refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terms	Definition
Terrorist act	A *terrorist act* includes: (i) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and (ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 organisation to do or to abstain from doing any act.
Terrorist financing (FT)	*Terrorist financing (FT)* includes the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist Financing Convention	The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism
Terrorist financing offence	References in this Methodology (except in SR II) to a *terrorist financing (FT) offence* refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organisation	For purposes of SRIII, the term *terrorist organisation* is as defined in the Interpretative Note of SRIII. Otherwise, it refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	*For the purposes of R.9 only*, *third parties* means financial institutions or DNFBP that are supervised and that meet Criteria 9.1 to 9.4
Those who finance terrorism	For the purposes of SR III only, the phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to

Terms	Definition
	facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets 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 terrorist acts.
Transactions	In the insurance sector, the word *transactions* should be understood to refer to the insurance product itself, the premium payment and the benefits. For specific requirements with regard to record keeping of transactions in the insurance sector, see the IAIS Guidance Notes of January 2002.
Trustee	*Trustees*, who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.
Unique identifier	For the purposes of Special Recommendation VII, a *unique identifier* refers to any unique combination of letters, numbers or symbols that refers to a specific originator.
Vienna Convention	The 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Pyschotropic Substances
Wire transfer	For the purposes of Special Recommendations VII, the terms *wire transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
Without delay	For the purposes of Special Recommendation III, the phrase *without delay* has the following specific meaning. For the purposes of S/RES/1267(1999), it means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. The phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Annex 2:
Endorsement of the AML/CFT Methodology 2004

This Methodology was agreed by the FATF Plenary at its meeting in February 2004, and approved by the Executive Boards of the IMF and the World Bank in March 2004. The following bodies have also endorsed the Methodology: the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Eurasian Group (EAG), the Financial Action Task Force on Money Laundering in South America (GAFISUD), the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), the Middle East and North Africa Financial Action Task Force (MENAFATF) and the Offshore Group of Banking Supervisors (OGBS).

Annex 3:
Information on updates made to the 2004 Methodology

The tables below identify the amendments made to the Methodology since its adoption in February 2004. Editorial amendments (as opposed to substantive amendments) are intended to ensure that the Methodology accurately reflects the Recommendations and have no impact on the substance of the requirements. Technical amendments refer to amendments made to reflect the changes made to the standards themselves (including amendments made to Interpretative Notes), to correct some minor mistakes when transposing the Recommendations or to avoid a duplication of assessment of individual Recommendations in the evaluation process.

1. Editorial amendments

Date	Section of the Methodology subject to amendments
February 2005	▪ Introduction ▪ R.5 – C.5.15

2. Technical amendments

Date	Type of amendments	Sections subject to amendments
February 2005	Introduction of a new set of criteria in relation to SRIX and its Interpretative Note adopted	▪ R.19 – all references to cross-border transportation of currency and bearer negotiable instruments deleted (C.19.1 & C.19.3 deleted, C. 19.2 – new C.19.1- & additional elements unchanged) ▪ SRIX –a complete set of criteria is introduced ▪ Glossary: adoption of new definitions for (1) *bearer negotiable instrument*; (2) *false declaration*; (3) *false disclosure*; (4) *physical cross-border transportation* and (5) *related to terrorist financing or money laundering*
	Update of Annex 2	▪ Annex 2 set out that APG, CFATF, MONEYVAL, ESSAMLG, GAFISUD and OGBS have endorsed the 2004 Methodology.
October 2005	Amendment to the treatment of sanctions for DNFBPs to avoid multiple-counting of the same issue	▪ C.12.3 deleted ▪ C.16.4 deleted ▪ *17.2* reference to *"the self-regulatory organisations referred to in Recommendation 24"* deleted ▪ *24.2.1 a)* reference to *"criteria 17.1-17.4 that apply to the obligations under R.12 and R.16"* added
	Align the Methodology with changes made to the Interpretative Note on SR VII	▪ note to assessors deleted ▪ Chapeau to essential criteria amended – reference to *withdrawals from a bank account through an ATM machine, cash advances from a credit card, or payments for goods and services* added. ▪ *C.VII.1& C.VII.2:* EUR/USD 1 000 or more threshold introduced ▪ *C.VII.2*: provisions in relation to batch transfers amended – previous provisions deleted ▪ *C.VII.3*: reference to *transactions using a credit or debit card* deleted ▪ *C.VII.4* – previous provisions on routine batch transfers deleted

Date	Type of amendments	Sections subject to amendments
		– new criterion introduced provision related to the obligation to maintain originator information (previous C.VII.5) ▪ *C.VII.5* – new criterion introduced provision on effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information ▪ two additional elements introduced provisions on incoming & outgoing cross-border wire transfers ▪ Glossary – adoption of definition of *unique identifier*
June 2006	Introduction – additional element s on corruption Align the Methodology with changes made to the Interpretative Note on SR VII Align the Methodology with the new Interpretative Note on SRVIII	▪ Paragraph 7c) – elements on anti-corruption initiatives added ▪ Chapeau*:* reference to Criterion 5.2 deleted ▪ *C. VII.1* – the verification element amended ▪ Footnote of C.*VII.*1 amended ▪ A complete set of essential and additional criteria adopted. C.VIII.1 to C.VIII.4 of Methodology (version February 2004) deleted. ▪ Glossary: adoption of new definitions for (1*)* *appropriate authorities*; (2) *associate NPOs*; (3) *beneficiary*; (4) *non-profit organisation.*
February 2007	Introduction – note to additional elements on effectiveness Insert notes for assessors on interpretation of the FATF Recommendations Insertion of Annex 3	▪ Paragraph 6 – elements on global effectiveness added ▪ New paragraphs 15 to 18 – elements on the measure of effectiveness of implementation of individual recommendations added ▪ Rec. 1, Rec. 2, SRII, Rec. 12, Rec. 36, 38, 39 & SRV and SRVI ▪ Information on updates made to the 2004 Methodology added
February 2008	Introduction – insert note to assessors on the basic requirements that have to be met for a measure to be considered as “other enforceable means” SRVII & Glossary – amend the definition of “domestic transfer”.	▪ Paragraph 24 – “Note to assessors” added in relation to the definition of “other enforceable means” ▪ Definition of “domestic transfer” is amended and an explanatory note is added in C.VII.3.

Date	Type of amendments	Sections subject to amendments
October 2008	Introduction – add text Make Methodology more in line with UN Conventions on ancillary offences	▪ insert new paragraphs 16-18 addressing issue of effectiveness and upgrading for financial institution preventive measures. • C.1.7 – add reference to "association with" as alternative ancillary offence to conspiracy. Add footnote to C.1.7
February 2009	SR IX – amendments of the Essential Criteria	• Addition to a supra-national approach to SR.IX (especially in C.IX.4, C.IX.5, C.IX.7 and C.IX.13) • Two new essential criteria: C.IX.14 and C.IX.15.

FATF/OECD
April 2009

www.fatf-gafi.org

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Descriptive and Mann-Whitney Test (by nature of work)

Question 1 – What is the effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing?

Part One

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Valid	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00
Mean	4.81	4.88	4.20	2.99	4.12	4.34	4.80	4.73	4.61	4.66	4.57	3.62	4.85	4.96
Median	5.00	5.00	4.00	3.00	4.00	4.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00	5.00
Mode	5.00	5.00	5.00	3.00	4.00	4.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00	5.00
Std. Deviation	0.39	0.33	0.86	0.97	0.88	0.56	0.40	0.45	0.49	0.48	0.58	1.39	0.36	0.20

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
		Mean Rank													
Uniformed	39	37.9	38.2	35.2	36.4	38.8	36.9	39.3	38.0	40.6	37.7	38.9	38.0	34.5	38.1
Civilian	35	37.1	36.7	40.0	38.8	36.0	38.2	35.5	36.9	34.0	37.3	36.0	36.9	40.9	36.9
Mann-Whitney U statistic		668.5	655	593.5	638.5	631	658.5	612	662.5	561	676	629	662	564	661
Z		-0.22	-0.53	-1.05	-0.50	-0.60	-0.30	-1.10	-0.28	-1.56	-0.09	-0.68	-0.24	-2.08	-0.68
p-value		0.823	0.599	0.296	0.617	0.550	0.764	0.273	0.778	0.120	0.932	0.494	0.814	0.037	0.496

Part Two

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Valid	74.00	74.00	74.00	74.00	74.00	74.00	74.00	74.00
Mean	4.97	4.88	4.22	4.36	4.55	4.92	4.89	3.73
Median	5.00	5.00	4.00	4.00	5.00	5.00	5.00	4.00
Mode	5.00	5.00	4.00	4.00	5.00	5.00	5.00	5.00
Std. Deviation	0.16	0.33	0.67	0.61	0.55	0.27	0.31	1.47

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
		Mean Rank							
Uniformed	39	37.6	37.3	36.7	41.2	39.7	37.7	34.9	37.0
Civilian	35	37.4	37.8	38.4	33.4	35.1	37.3	40.4	38.1
Mann-Whitney U statistic		681	673	651	540	598	677	580	662
Z		-0.08	-0.18	-0.38	-1.73	-1.07	-0.14	-2.07	-0.24
p-value		0.939	0.856	0.702	0.083	0.286	0.891	0.038	0.811

Part Three

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Valid	74.00	74.00	74.00	74.00	74.00	74.00	74.00
Mean	4.97	4.92	4.30	4.45	4.30	4.04	4.59
Median	5.00	5.00	4.00	4.00	4.00	4.00	5.00
Mode	5.00	5.00	4.00	5.00	4.00	5.00	5.00
Std. Deviation	0.16	0.27	0.66	0.58	0.68	1.14	0.49

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7
		Mean Rank						
Uniformed	39	36.6	36.7	35.8	35.9	35.7	37.3	36.4
Civilian	35	38.5	38.4	39.4	39.3	39.5	37.7	38.8
Mann-Whitney U statistic		648	652	617	621	612	674	639
Z		-1.35	-0.71	-0.79	-0.75	-0.84	-0.10	-0.56
p-value		0.177	0.478	0.429	0.451	0.402	0.921	0.575

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Question Two – What is the effectiveness of SAFIU in administering money laundering and terrorism financing crimes with other governmental and non-governmental agencies such as finance and banking institutions?

Part One

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Mean	3.93	4.34	5.00	4.31	4.91	4.31	4.86	4.96	3.85	4.41	4.57	4.97	5.00	4.84	4.32	3.89	4.15	4.03
Median	4.00	4.00	5.00	4.00	5.00	4.00	5.00	5.00	4.00	4.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00	5.00
Mode	4.00	4.00	5.00	4.00	5.00	4.00	5.00	5.00	4.00	4.00	5.00	5.00	5.00	5.00	5.00	4.00	5.00	5.00
Std. Deviation	0.56	0.48	0.00	0.66	0.29	0.52	0.34	0.20	0.68	0.55	0.86	0.16	0.00	0.37	1.30	1.32	1.36	1.63

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
		Mean rank																	
Uniformed	39	35.6	38.3	37.5	34.8	37.2	39.8	38.7	37.1	40.2	35.3	35.8	36.6	37.5	35.0	36.4	36.8	36.2	38.2
Civilian	35	39.6	36.6	37.5	40.5	37.8	34.9	36.2	37.9	34.5	40.0	39.4	38.5	37.5	40.3	38.7	38.3	39.0	36.7
Mann-Whitney U statistic		608	652	683	577	671	591	636	667	576	596	617	648	683	584	640	655	630	654
Z		-1.00	-0.40	0.00	-1.26	-0.25	-1.18	-0.86	-0.49	-1.53	-1.08	-0.96	-1.35	0.00	-1.68	-0.61	-0.32	-0.66	-0.38
p-value		0.32	0.69	1.00	0.21	0.81	0.24	0.39	0.62	0.12	0.28	0.33	0.18	1.00	0.09	0.54	0.75	0.51	0.70

Part Two

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Mean	4.39	4.43	4.97	4.69	4.53	4.35	4.39	4.12	4.77
Median	4.00	4.00	5.00	5.00	5.00	4.00	4.00	4.00	5.00
Mode	4.00	4.00	5.00	5.00	5.00	4.00	4.00	4.00	5.00
Std. Deviation	0.49	0.50	0.16	0.62	1.04	0.65	0.62	0.96	0.59

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
		Mean Rank								
Uniformed	39	38.18	37.63	36.60	36.41	36.78	36.47	38.27	36.33	36.47
Civilian	35	36.74	37.36	38.50	38.71	38.30	38.64	36.64	38.80	38.64
Mann-Whitney U statistic		656	678	648	640	655	643	653	637	643
Z		-.339	-.063	-1.349	-.627	-.432	-.480	-.364	-.534	-.701
p-value		.73	.95	.18	.53	.67	.63	.72	.59	.48

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Question Three – What is the effectiveness of the international cooperation of anti-money laundering and terrorism finance combating between SAFIU and FIUs in other countries?

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	4.15	4.93	4.41	4.45	4.47	4.57	3.39	3.39	3.39	4.88
Median	5.00	5.00	4.00	4.00	4.00	5.00	4.00	4.00	4.00	5.00
Mode	5.00	5.00	4.00	4.00	4.00	5.00	4.00	4.00	4.00	5.00
Std. Deviation	1.09	0.25	0.55	0.50	0.50	0.50	1.29	1.28	1.28	0.33

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
		Mean Rank									
Uniformed	39	36.9	37.2	36.7	37.1	35.2	36.4	35.6	36.2	35.4	36.3
Civilian	35	38.2	37.9	38.4	37.9	40.1	38.7	39.6	38.9	39.8	38.8
Mann-Whitney U statistic		659	669	652.5	668	592	640.5	608.5	633.5	601	636
Z		-0.28	-0.34	-0.37	-0.18	-1.13	-0.53	-0.88	-0.59	-0.97	-0.89
p-value		0.78	0.74	0.71	0.86	0.26	0.60	0.38	0.55	0.33	0.37

Question Four - What suggestions can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism financing activities?

Descriptive statistics

	Q1	Q2	Q3	Q4	Q5	Q6
Mean	5.00	4.81	4.95	4.50	4.54	4.59
Median	5.00	5.00	5.00	4.50	5.00	5.00
Mode	5.00	5.00	5.00	4.00	5.00	5.00
Std. Deviation	0.00	0.39	0.23	0.50	0.50	0.49

Mann-Whitney U Test

	N	Q1	Q2	Q3	Q4	Q5	Q6
		Mean Rank					
Uniformed	39	37.50	37.86	37.60	37.97	38.37	35.42
Civilian	35	37.50	37.10	37.39	36.97	36.53	39.81
Mann-Whitney U statistic		683	669	679	664	649	602
Z		.000	-.223	-.111	-.231	-.426	-1.031
p-value		1.000	.823	.912	.817	.670	.302

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Correlation Statistics (Spearman's Rho)

Question One - What is the effectiveness of SAFIU in receiving and analysing STRs on money laundering and terrorism financing?

Part One

			Correlations Spearman's rho												
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
Q1	Correlation Coefficient	1.00	0.77	0.62	-0.25	-0.16	0.24	-0.16	-0.29	-0.18	-0.35	-0.15	0.38	-0.10	-0.10
	Sig. (1-tailed)		**0.00**	**0.00**	**0.02**	0.08	**0.02**	0.09	**0.01**	0.07	**0.00**	0.09	**0.00**	0.19	0.20
Q2	Correlation Coefficient	0.77	1.00	0.46	-0.46	-0.37	0.22	-0.19	-0.23	-0.30	-0.27	-0.30	0.16	-0.16	-0.08
	Sig. (1-tailed)	**0.00**		**0.00**	**0.00**	**0.00**	**0.03**	**0.05**	**0.03**	**0.00**	**0.01**	**0.01**	0.09	0.09	0.26
Q3	Correlation Coefficient	0.62	0.46	1.00	0.03	0.03	0.34	-0.27	-0.34	-0.01	-0.21	0.10	0.59	0.01	0.14
	Sig. (1-tailed)	**0.00**	**0.00**		0.39	0.41	**0.00**	**0.01**	**0.00**	0.47	**0.04**	0.19	**0.00**	0.45	0.11
Q4	Correlation Coefficient	-0.25	-0.46	0.03	1.00	0.29	0.10	0.19	0.17	0.12	0.20	0.47	0.27	0.01	0.04
	Sig. (1-tailed)	**0.02**	**0.00**	0.39		**0.01**	0.20	0.06	0.08	0.16	**0.04**	**0.00**	**0.01**	0.46	0.37
Q5	Correlation Coefficient	-0.16	-0.37	0.03	0.29	1.00	0.11	0.16	0.19	0.30	0.31	0.20	0.10	0.23	0.06
	Sig. (1-tailed)	0.08	**0.00**	0.41	**0.01**		0.17	0.09	**0.05**	**0.00**	**0.00**	**0.05**	0.19	**0.02**	0.29
Q6	Correlation Coefficient	0.24	0.22	0.34	0.10	0.11	1.00	-0.18	-0.17	-0.11	0.04	0.18	0.34	0.04	0.09
	Sig. (1-tailed)	**0.02**	**0.03**	**0.00**	0.20	0.17		0.07	0.07	0.17	0.35	0.06	**0.00**	0.37	0.22
Q7	Correlation Coefficient	-0.16	-0.19	-0.27	0.19	0.16	-0.18	1.00	0.60	0.15	0.07	0.12	-0.13	0.07	-0.10
	Sig. (1-tailed)	0.09	**0.05**	**0.01**	0.06	0.09	0.07		**0.00**	0.11	0.29	0.15	0.14	0.27	0.19
Q8	Correlation Coefficient	-0.29	-0.23	-0.34	0.17	0.19	-0.17	0.60	1.00	0.32	0.27	0.05	-0.40	0.00	-0.13
	Sig. (1-tailed)	**0.01**	**0.03**	**0.00**	0.08	**0.05**	0.07	**0.00**		**0.00**	**0.01**	0.34	**0.00**	0.49	0.14
Q9	Correlation Coefficient	-0.18	-0.30	-0.01	0.12	0.30	-0.11	0.15	0.32	1.00	0.36	0.11	0.02	-0.02	0.12
	Sig. (1-tailed)	0.07	**0.00**	0.47	0.16	**0.00**	0.17	0.11	**0.00**		**0.00**	0.18	0.44	0.42	0.16
Q10	Correlation Coefficient	-0.35	-0.27	-0.21	0.20	0.31	0.04	0.07	0.27	0.36	1.00	0.23	-0.20	0.10	-0.15
	Sig. (1-tailed)	**0.00**	**0.01**	**0.04**	**0.04**	**0.00**	0.35	0.29	**0.01**	**0.00**		**0.02**	0.05	0.19	0.11
Q11	Correlation Coefficient	-0.15	-0.30	0.10	0.47	0.20	0.18	0.12	0.05	0.11	0.23	1.00	0.28	0.11	0.16
	Sig. (1-tailed)	0.09	**0.01**	0.19	**0.00**	**0.05**	0.06	0.15	0.34	0.18	**0.02**		**0.01**	0.17	0.09
Q12	Correlation Coefficient	0.38	0.16	0.59	0.27	0.10	0.34	-0.13	-0.40	0.02	-0.20	0.28	1.00	0.08	0.09
	Sig. (1-tailed)	**0.00**	0.09	**0.00**	**0.01**	0.19	**0.00**	0.14	**0.00**	0.44	**0.05**	**0.01**		0.25	0.22
Q13	Correlation Coefficient	-0.10	-0.16	0.01	0.01	0.23	0.04	0.07	0.00	-0.02	0.10	0.11	0.08	1.00	-0.09
	Sig. (1-tailed)	0.19	0.09	0.45	0.46	**0.02**	0.37	0.27	0.49	0.42	0.19	0.17	0.25		0.23
Q14	Correlation Coefficient	-0.10	-0.08	0.14	0.04	0.06	0.09	-0.10	-0.13	0.12	-0.15	0.16	0.09	-0.09	1.00
	Sig. (1-tailed)	0.20	0.26	0.11	0.37	0.29	0.22	0.19	0.14	0.16	0.11	0.09	0.22	0.23	

Part Two

Correlations Spearman's rho									
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Q1	Correlation Coefficient	1.00	-0.06	0.17	0.21	0.09	0.26	0.48	0.25
	Sig. (1-tailed)		0.30	0.07	**0.04**	0.22	**0.01**	**0.00**	**0.02**
Q2	Correlation Coefficient	-0.06	1.00	0.15	-0.11	-0.15	0.04	0.14	0.29
	Sig. (1-tailed)	0.30		0.10	0.17	0.10	0.36	0.12	**0.01**
Q3	Correlation Coefficient	0.17	0.15	1.00	0.17	0.05	0.00	0.09	0.41
	Sig. (1-tailed)	**0.07**	0.10		**0.07**	0.33	0.50	0.22	**0.00**
Q4	Correlation Coefficient	0.21	-0.11	0.17	1.00	0.40	0.09	0.14	0.31
	Sig. (1-tailed)	**0.04**	0.17	0.07		**0.00**	0.23	0.12	**0.00**
Q5	Correlation Coefficient	0.09	-0.15	0.05	0.40	1.00	-0.11	0.00	0.18
	Sig. (1-tailed)	0.22	0.10	0.33	**0.00**		0.17	0.50	0.06
Q6	Correlation Coefficient	0.26	0.04	0.00	0.09	-0.11	1.00	0.53	0.32
	Sig. (1-tailed)	**0.01**	0.36	0.50	0.23	0.17		**0.00**	**0.00**
Q7	Correlation Coefficient	0.48	0.14	0.09	0.14	0.00	0.53	1.00	0.44
	Sig. (1-tailed)	**0.00**	0.12	0.22	0.12	0.50	**0.00**		**0.00**
Q8	Correlation Coefficient	0.25	0.29	0.41	0.31	0.18	0.32	0.44	1.00
	Sig. (1-tailed)	**0.02**	**0.01**	**0.00**	**0.00**	0.06	**0.00**	**0.00**	

Part Three

	Correlations Spearman's rho							
		Q1	Q2	Q3	Q4	Q5	Q6	Q7
Q1	Correlation Coefficient	1.00	0.26	0.19	-0.01	0.28	0.27	0.03
	Sig. (1-tailed)		**0.01**	**0.05**	0.46	**0.01**	**0.01**	0.39
Q2	Correlation Coefficient	0.26	1.00	0.11	0.07	0.39	0.44	0.16
	Sig. (1-tailed)	**0.01**		0.17	0.27	**0.00**	**0.00**	0.09
Q3	Correlation Coefficient	0.19	0.11	1.00	0.21	0.20	0.43	0.30
	Sig. (1-tailed)	**0.05**	0.17		**0.03**	**0.05**	**0.00**	**0.00**
Q4	Correlation Coefficient	-0.01	0.07	0.21	1.00	0.16	0.21	0.00
	Sig. (1-tailed)	0.46	0.27	**0.03**		0.08	**0.04**	0.50
Q5	Correlation Coefficient	0.28	0.39	0.20	0.16	1.00	0.48	0.16
	Sig. (1-tailed)	**0.01**	**0.00**	**0.05**	0.08		**0.00**	0.09
Q6	Correlation Coefficient	0.27	0.44	0.43	0.21	0.48	1.00	0.48
	Sig. (1-tailed)	**0.01**	**0.00**	**0.00**	**0.04**	**0.00**		**0.00**
Q7	Correlation Coefficient	0.03	0.16	0.30	0.00	0.16	0.48	1.00
	Sig. (1-tailed)	0.39	0.09	**0.00**	0.50	0.09	**0.00**	

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Question Two – What is the effectiveness of SAFIU in administering money laundering and terrorism financing crimes with other governmental and non-governmental agencies such as finance and banking institutions?

Part One

		Correlations Spearman's rho																	
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Q1	Correlation Coefficient	1.00	0.18		0.33	0.05	-0.01	0.32	-0.03	0.19	0.29	0.40	-0.02		0.28	0.46	0.30	0.31	0.42
	Sig. (1-tailed)		0.06		0.00	0.35	0.45	0.00	0.40	0.05	0.01	0.00	0.42		0.01	0.00	0.01	0.00	0.00
Q2	Correlation Coefficient	0.18	1.00		-0.05	-0.06	0.06	-0.05	-0.14	0.05	0.11	0.00	-0.23		0.08	-0.05	-0.01	-0.14	-0.05
	Sig. (1-tailed)	0.06			0.34	0.30	0.31	0.33	0.11	0.33	0.17	0.50	0.02		0.24	0.32	0.48	0.12	0.33
Q3	Correlation Coefficient																		
Q4	Correlation Coefficient	0.33	-0.05		1.00	0.27	0.26	0.12	0.20	0.32	0.03	0.50	0.10		0.40	0.53	0.42	0.51	0.48
	Sig. (1-tailed)	0.00	0.34			0.01	0.01	0.15	0.05	0.00	0.41	0.00	0.20		0.00	0.00	0.00	0.00	0.00
Q5	Correlation Coefficient	0.05	-0.06		0.27	1.00	0.27	0.14	0.40	0.16	0.08	0.38	0.23		0.23	0.38	0.26	0.36	0.32
	Sig. (1-tailed)	0.35	0.30		0.01		0.01	0.11	0.00	0.09	0.24	0.00	0.02		0.02	0.00	0.01	0.00	0.00
Q6	Correlation Coefficient	-0.01	0.06		0.26	0.27	1.00	0.23	-0.01	0.15	0.11	0.26	-0.06		0.18	0.23	0.29	0.30	0.31
	Sig. (1-tailed)	0.45	0.31		0.01	0.01		0.03	0.48	0.11	0.17	0.01	0.30		0.06	0.02	0.01	0.00	0.00
Q7	Correlation Coefficient	0.32	-0.05		0.12	0.14	0.23	1.00	-0.08	-0.05	0.06	0.24	-0.07		0.15	0.30	0.07	0.26	0.26
	Sig. (1-tailed)	0.00	0.33		0.15	0.11	0.03		0.25	0.33	0.31	0.02	0.29		0.10	0.00	0.27	0.01	0.01
Q8	Correlation Coefficient	-0.03	-0.14		0.20	0.40	-0.01	-0.08	1.00	-0.03	0.17	0.19	0.39		0.10	0.23	0.03	0.28	0.29
	Sig. (1-tailed)	0.40	0.11		0.05	0.00	0.48	0.25		0.39	0.08	0.05	0.00		0.21	0.02	0.41	0.01	0.01
Q9	Correlation Coefficient	0.19	0.05		0.32	0.16	0.15	-0.05	-0.03	1.00	0.21	0.39	-0.19		0.26	0.31	0.37	0.31	0.45
	Sig. (1-tailed)	0.05	0.33		0.00	0.09	0.11	0.33	0.39		0.04	0.00	0.05		0.01	0.00	0.00	0.00	0.00
Q10	Correlation Coefficient	0.29	0.11		0.03	0.08	0.11	0.06	0.17	0.21	1.00	0.27	-0.03		0.30	0.24	0.25	0.28	0.39
	Sig. (1-tailed)	0.01	0.17		0.41	0.24	0.17	0.31	0.08	0.04		0.01	0.41		0.01	0.02	0.02	0.01	0.00
Q11	Correlation Coefficient	0.40	0.00		0.50	0.38	0.26	0.24	0.19	0.39	0.27	1.00	0.31		0.81	0.85	0.74	0.77	0.83
	Sig. (1-tailed)	0.00	0.50		0.00	0.00	0.01	0.02	0.05	0.00	0.01		0.00		0.00	0.00	0.00	0.00	0.00
Q12	Correlation Coefficient	-0.02	-0.23		0.10	0.23	-0.06	-0.07	0.39	-0.19	-0.03	0.31	1.00		0.38	0.30	0.14	0.27	0.27
	Sig. (1-tailed)	0.42	0.02		0.20	0.02	0.30	0.29	0.00	0.05	0.41	0.00			0.00	0.00	0.12	0.01	0.01
Q13	Correlation Coefficient																		
Q14	Correlation Coefficient	0.28	0.08		0.40	0.23	0.18	0.15	0.10	0.26	0.30	0.81	0.38		1.00	0.73	0.63	0.69	0.72
	Sig. (1-tailed)	0.01	0.24		0.00	0.02	0.06	0.10	0.21	0.01	0.01	0.00	0.00			0.00	0.00	0.00	0.00
Q15	Correlation Coefficient	0.46	-0.05		0.53	0.38	0.23	0.30	0.23	0.31	0.24	0.85	0.30		0.73	1.00	0.63	0.75	0.79
	Sig. (1-tailed)	0.00	0.32		0.00	0.00	0.02	0.00	0.02	0.00	0.02	0.00	0.00		0.00		0.00	0.00	0.00
Q16	Correlation Coefficient	0.30	-0.01		0.42	0.26	0.29	0.07	0.03	0.37	0.25	0.74	0.14		0.63	0.63	1.00	0.60	0.67
	Sig. (1-tailed)	0.01	0.48		0.00	0.01	0.01	0.27	0.41	0.00	0.02	0.00	0.12		0.00	0.00		0.00	0.00
Q17	Correlation Coefficient	0.31	-0.14		0.51	0.36	0.30	0.26	0.28	0.31	0.28	0.77	0.27		0.69	0.75	0.60	1.00	0.82
	Sig. (1-tailed)	0.00	0.12		0.00	0.00	0.00	0.01	0.01	0.00	0.01	0.00	0.01		0.00	0.00	0.00		0.00
Q18	Correlation Coefficient	0.42	-0.05		0.48	0.32	0.31	0.26	0.29	0.45	0.39	0.83	0.27		0.72	0.79	0.67	0.82	1.00
	Sig. (1-tailed)	0.00	0.33		0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.01		0.00	0.00	0.00	0.00	

Part Two

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Q1	Correlation Coefficient	1.00	0.42	-0.04	-0.02	0.06	0.03	0.16	0.21	0.03
	Sig. (1-tailed)		0.00	0.38	0.45	0.29	0.42	0.08	0.04	0.41
Q2	Correlation Coefficient	0.42	1.00	0.15	0.24	0.23	0.24	0.10	0.28	0.14
	Sig. (1-tailed)	0.00		0.11	0.02	0.03	0.02	0.20	0.01	0.11
Q3	Correlation Coefficient	-0.04	0.15	1.00	0.32	0.14	0.06	0.21	0.24	0.18
	Sig. (1-tailed)	0.38	0.11		0.00	0.11	0.32	0.03	0.02	0.06
Q4	Correlation Coefficient	-0.02	0.24	0.32	1.00	0.92	0.45	0.29	0.64	0.76
	Sig. (1-tailed)	0.45	0.02	0.00		0.00	0.00	0.01	0.00	0.00
Q5	Correlation Coefficient	0.06	0.23	0.14	0.92	1.00	0.52	0.25	0.64	0.86
	Sig. (1-tailed)	0.29	0.03	0.11	0.00		0.00	0.02	0.00	0.00
Q6	Correlation Coefficient	0.03	0.24	0.06	0.45	0.52	1.00	0.24	0.50	0.42
	Sig. (1-tailed)	0.42	0.02	0.32	0.00	0.00		0.02	0.00	0.00
Q7	Correlation Coefficient	0.16	0.10	0.21	0.29	0.25	0.24	1.00	0.34	0.19
	Sig. (1-tailed)	0.08	0.20	0.03	0.01	0.02	0.02		0.00	0.05
Q8	Correlation Coefficient	0.21	0.28	0.24	0.64	0.64	0.50	0.34	1.00	0.54
	Sig. (1-tailed)	0.04	0.01	0.02	0.00	0.00	0.00	0.00		0.00
Q9	Correlation Coefficient	0.03	0.14	0.18	0.76	0.86	0.42	0.19	0.54	1.00
	Sig. (1-tailed)	0.41	0.11	0.06	0.00	0.00	0.00	0.05	0.00	

APPENDIX C

Descriptive Statistics, Mann-Whitney Test (by nature of work) and Correlations Statistics

Question Three – What is the effectiveness of the international cooperation of anti-money laundering and terrorism finance combating between SAFIU and FIUs in other countries?

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Q1	Correlation Coefficient	1.00	0.27	0.19	-0.07	0.25	0.09	0.29	0.28	0.31	0.37
	Sig. (1-tailed)		0.01	0.05	0.28	0.02	0.23	0.01	0.01	0.00	0.00
Q2	Correlation Coefficient	0.27	1.00	0.17	-0.08	0.15	0.09	0.24	0.29	0.23	0.23
	Sig. (1-tailed)	0.01		0.07	0.24	0.11	0.22	0.02	0.01	0.03	0.02
Q3	Correlation Coefficient	0.19	0.17	1.00	0.30	0.23	0.00	0.45	0.43	0.41	0.15
	Sig. (1-tailed)	0.05	0.07		0.01	0.02	0.49	0.00	0.00	0.00	0.10
Q4	Correlation Coefficient	-0.07	-0.08	0.30	1.00	-0.03	0.01	0.20	0.17	0.20	0.17
	Sig. (1-tailed)	0.28	0.24	0.01		0.39	0.45	0.04	0.07	0.04	0.08
Q5	Correlation Coefficient	0.25	0.15	0.23	-0.03	1.00	0.01	0.21	0.25	0.21	0.27
	Sig. (1-tailed)	0.02	0.11	0.02	0.39		0.48	0.04	0.02	0.04	0.01
Q6	Correlation Coefficient	0.09	0.09	0.00	0.01	0.01	1.00	-0.09	-0.03	-0.06	0.09
	Sig. (1-tailed)	0.23	0.22	0.49	0.45	0.48		0.23	0.40	0.30	0.22
Q7	Correlation Coefficient	0.29	0.24	0.45	0.20	0.21	-0.09	1.00	0.95	0.97	0.28
	Sig. (1-tailed)	0.01	0.02	0.00	0.04	0.04	0.23		0.00	0.00	0.01
Q8	Correlation Coefficient	0.28	0.29	0.43	0.17	0.25	-0.03	0.95	1.00	0.95	0.34
	Sig. (1-tailed)	0.01	0.01	0.00	0.07	0.02	0.40	0.00		0.00	0.00
Q9	Correlation Coefficient	0.31	0.23	0.41	0.20	0.21	-0.06	0.97	0.95	1.00	0.26
	Sig. (1-tailed)	0.00	0.03	0.00	0.04	0.04	0.30	0.00	0.00		0.01
Q10	Correlation Coefficient	0.37	0.23	0.15	0.17	0.27	0.09	0.28	0.34	0.26	1.00
	Sig. (1-tailed)	0.00	0.02	0.10	0.08	0.01	0.22	0.01	0.00	0.01	

Question Four - What suggestions can be provided to SAFIU to enable them to develop policies that better detect and combat money laundering and terrorism financing activities?

		Q1	Q2	Q3	Q4	Q5	Q6
Q1	Correlation Coefficient						
Q2	Correlation Coefficient		1.00	0.34	0.07	-0.03	0.09
	Sig. (1-tailed)			0.00	0.28	0.40	0.22
Q3	Correlation Coefficient		0.34	1.00	0.00	-0.10	0.05
	Sig. (1-tailed)		0.00		0.50	0.20	0.35
Q4	Correlation Coefficient		0.07	0.00	1.00	-0.05	0.44
	Sig. (1-tailed)		0.28	0.50		0.32	0.00
Q5	Correlation Coefficient		-0.03	-0.10	-0.05	1.00	0.07
	Sig. (1-tailed)		0.40	0.20	0.32		0.28
Q6	Correlation Coefficient		0.09	0.05	0.44	0.07	1.00
	Sig. (1-tailed)		0.22	0.35	0.00	0.28	

APPENDIX D
Findings of the Kruskal-Wallis Test

Age

	Age			Statistic	Std. Error
SAFIU receives money laundering and terrorism finance STRs through various channels.	Less than 30 years old	Mean		4.71	.087
		95% Confidence Interval for Mean	Lower Bound	4.54	
			Upper Bound	4.89	
	From 30 to less than 40 years old	Mean		4.97	.034
		95% Confidence Interval for Mean	Lower Bound	4.89	
			Upper Bound	5.04	
SAFIU collects information about suspicious and fictitious companies and institutions.	Less than 30 years old	Mean		4.36	.187
		95% Confidence Interval for Mean	Lower Bound	3.97	
			Upper Bound	4.74	
	From 30 to less than 40 years old	Mean		3.97	.145
		95% Confidence Interval for Mean	Lower Bound	3.67	
			Upper Bound	4.26	
	From 40 to less than 50 years old	Mean		3.93	.206
		95% Confidence Interval for Mean	Lower Bound	3.49	
			Upper Bound	4.38	
	From 50 years old and over	Mean		4.50	.500
		95% Confidence Interval for Mean	Lower Bound	-1.85	
			Upper Bound	10.85	
SAFIU exchanged information with other FIUs prior to joining Egmont Group.	Less than 30 years old	Mean		3.79	.226
		95% Confidence Interval for Mean	Lower Bound	3.32	
			Upper Bound	4.25	
	From 30 to less than 40 years old	Mean		4.17	.172
		95% Confidence Interval for Mean	Lower Bound	3.82	
			Upper Bound	4.53	
	From 40 to less than 50 years old	Mean		4.67	.270
		95% Confidence Interval for Mean	Lower Bound	4.09	
			Upper Bound	5.25	
SAFIU should operate their offices in major cities.	Less than 30 years old	Mean		4.29	.087
		95% Confidence Interval for Mean	Lower Bound	4.11	
			Upper Bound	4.46	
	From 30 to less than 40 years old	Mean		4.48	.094
		95% Confidence Interval for Mean	Lower Bound	4.29	
			Upper Bound	4.68	
	From 40 to less than 50 years old	Mean		4.87	.091
		95% Confidence Interval for Mean	Lower Bound	4.67	
			Upper Bound	5.06	
SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Less than 30 years old	Mean		4.32	.090
		95% Confidence Interval for Mean	Lower Bound	4.14	
			Upper Bound	4.51	
	From 30 to less than 40 years old	Mean		4.69	.087
		95% Confidence Interval for Mean	Lower Bound	4.51	
			Upper Bound	4.87	

	From 40 to less than 50 years old	Mean		4.87	.091
		95% Confidence Interval for Mean	Lower Bound	4.67	
			Upper Bound	5.06	

Scientific qualification

	Scientific qualification			Statistic	Std. Error
SAFIU requests money laundering and terrorist finance STRs from financial and non-financial institutions.	Secondary or less	Mean		4.33	.211
		95% Confidence Interval for Mean	Lower Bound	3.79	
			Upper Bound	4.88	
	Diploma	Mean		4.81	.088
		95% Confidence Interval for Mean	Lower Bound	4.63	
			Upper Bound	4.99	
	Bachelor	Mean		4.86	.052
		95% Confidence Interval for Mean	Lower Bound	4.76	
			Upper Bound	4.97	
SAFIU is authorised to request additional information on money laundering and terrorism financing STRs from financial and non-financial institutions either directly or through another authority.	Secondary or less	Mean		4.50	.224
		95% Confidence Interval for Mean	Lower Bound	3.93	
			Upper Bound	5.07	
	Diploma	Mean		4.81	.088
		95% Confidence Interval for Mean	Lower Bound	4.63	
			Upper Bound	4.99	
	Bachelor	Mean		4.95	.032
		95% Confidence Interval for Mean	Lower Bound	4.89	
			Upper Bound	5.02	
SAFIU has standardised STR froms that capture all the required information.	Secondary or less	Mean		3.33	.211
		95% Confidence Interval for Mean	Lower Bound	2.79	
			Upper Bound	3.88	
	Diploma	Mean		4.10	.168
		95% Confidence Interval for Mean	Lower Bound	3.75	
			Upper Bound	4.45	
	Bachelor	Mean		4.34	.134
		95% Confidence Interval for Mean	Lower Bound	4.07	
			Upper Bound	4.61	
	Master	Mean		4.67	.333
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	6.10	
SAFIU receives and reviews STRs that are not related to money laundering and terrorism finance.	Secondary or less	Mean		3.17	.543
		95% Confidence Interval for Mean	Lower Bound	1.77	
			Upper Bound	4.56	
	Diploma	Mean		3.05	.189
		95% Confidence Interval for Mean	Lower Bound	2.65	
			Upper Bound	3.44	
	Bachelor	Mean		2.93	.154
		95% Confidence	Lower Bound	2.62	

APPENDIX D
Findings of the Kruskal-Wallis Test

		Interval for Mean	Upper Bound	3.24	

SAFIU has supervisors who are knowledgeable in analysing STRs.	Secondary or less	Mean		4.67	.211
		95% Confidence Interval for Mean	Lower Bound	4.12	
			Upper Bound	5.21	
	Diploma	Mean		4.95	.048
		95% Confidence Interval for Mean	Lower Bound	4.85	
			Upper Bound	5.05	
	Bachelor	Mean		4.86	.052
		95% Confidence Interval for Mean	Lower Bound	4.76	
			Upper Bound	4.97	

SAFIU provides additional training to all staff members.	Secondary or less	Mean		3.33	.333
		95% Confidence Interval for Mean	Lower Bound	2.48	
			Upper Bound	4.19	
	Diploma	Mean		4.48	.164
		95% Confidence Interval for Mean	Lower Bound	4.13	
			Upper Bound	4.82	
	Bachelor	Mean		3.89	.193
		95% Confidence Interval for Mean	Lower Bound	3.50	
			Upper Bound	4.28	
	Master	Mean		4.67	.333
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	6.10	
Information held by SAFIU is securely protected.	Diploma	Mean		4.67	.105
		95% Confidence Interval for Mean	Lower Bound	4.45	
			Upper Bound	4.89	
	Bachelor	Mean		4.64	.073
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.78	
	Master	Mean		4.67	.333
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	6.10	

SAFIU issues rules and regulations that detail the process of cooperation and coordination between government and non-government organizations.	Secondary or less	Mean		3.83	.167
		95% Confidence Interval for Mean	Lower Bound	3.40	
			Upper Bound	4.26	
	Diploma	Mean		4.52	.112
		95% Confidence Interval for Mean	Lower Bound	4.29	
			Upper Bound	4.76	
	Bachelor	Mean		4.23	.107
		95% Confidence Interval for Mean	Lower Bound	4.01	
			Upper Bound	4.44	
Businesses have awareness and knowledge of the danger of money laundering and the terrorism financing.	Secondary or less	Mean		3.00	.894
		95% Confidence Interval for Mean	Lower Bound	.70	
			Upper Bound	5.30	
	Diploma	Mean		4.76	.194

APPENDIX D
Findings of the Kruskal-Wallis Test

		95% Confidence Interval for Mean	Lower Bound	4.36	
			Upper Bound	5.17	
	Bachelor	Mean		3.75	.262
		95% Confidence Interval for Mean	Lower Bound	3.22	
			Upper Bound	4.28	

SAFIU exchanges information regarding money laundering and terrorism finance with other domestic government agencies	Secondary or less	Mean		4.67	.211
		95% Confidence Interval for Mean	Lower Bound	4.12	
			Upper Bound	5.21	
SAFIU cooperates with authorities in investigations that relate to money laundering and terrorism finance.	Secondary or less	Mean		4.33	.333
		95% Confidence Interval for Mean	Lower Bound	3.48	
			Upper Bound	5.19	
	Diploma	Mean		4.90	.095
		95% Confidence Interval for Mean	Lower Bound	4.71	
			Upper Bound	5.10	
	Bachelor	Mean		4.61	.099
		95% Confidence Interval for Mean	Lower Bound	4.41	
			Upper Bound	4.81	
SAFIU provides training programs to financial and nonfinancial institutions to understand money laundering and terrorism financing rules and regulations.	Secondary or less	Mean		3.67	.211
		95% Confidence Interval for Mean	Lower Bound	3.12	
			Upper Bound	4.21	
	Diploma	Mean		4.52	.164
		95% Confidence Interval for Mean	Lower Bound	4.18	
			Upper Bound	4.87	
	Bachelor	Mean		3.95	.159
		95% Confidence Interval for Mean	Lower Bound	3.63	
			Upper Bound	4.28	
	Master	Mean		4.67	.333
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	6.10	

SAFIU exchanged information with other FIUs prior to joining Egmont Group.	Secondary or less	Mean		2.67	.333
		95% Confidence Interval for Mean	Lower Bound	1.81	
			Upper Bound	3.52	
	Diploma	Mean		4.48	.164
		95% Confidence Interval for Mean	Lower Bound	4.13	
			Upper Bound	4.82	
	Bachelor	Mean		4.14	.171
		95% Confidence Interval for Mean	Lower Bound	3.79	
			Upper Bound	4.48	

SAFIU should operate their offices in major cities.	Diploma	Mean		4.62	.109
		95% Confidence Interval for Mean	Lower Bound	4.39	
			Upper Bound	4.85	
	Bachelor	Mean		4.48	.076
		95% Confidence Interval for Mean	Lower Bound	4.32	
			Upper Bound	4.63	

SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Secondary or less	Mean		4.17	.167
		95% Confidence Interval for Mean	Lower Bound	3.74	
			Upper Bound	4.60	
	Diploma	Mean		4.57	.111
		95% Confidence Interval for Mean	Lower Bound	4.34	
			Upper Bound	4.80	
	Bachelor	Mean		4.64	.073
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.78	

Years number of work experience

	Years number of work experience			Statistic	Std. Error
SAFIU is authorised to request additional information on money laundering and terrorist financing STRs from financial and non-financial institutions either directly or through anothet authority.	Less than 5 years	Mean		4.53	.125
		95% Confidence Interval for Mean	Lower Bound	4.26	
			Upper Bound	4.79	
	From 5 to less than 10 years	Mean		4.84	.065
		95% Confidence Interval for Mean	Lower Bound	4.71	
			Upper Bound	4.98	
	From 15 to less than 20 years	Mean		4.92	.083
		95% Confidence Interval for Mean	Lower Bound	4.73	
			Upper Bound	5.10	
SAFIU receives money laundering and terrorism finance STRs through various channels.	Less than 5 years	Mean		4.59	.123
		95% Confidence Interval for Mean	Lower Bound	4.33	
			Upper Bound	4.85	
	From 5 to less than 10 years	Mean		4.94	.043
		95% Confidence Interval for Mean	Lower Bound	4.85	
			Upper Bound	5.03	
SAFIU has standardised STR froms that capture all the required information.	Less than 5 years	Mean		3.71	.206
		95% Confidence Interval for Mean	Lower Bound	3.27	
			Upper Bound	4.14	
	From 5 to less than 10 years	Mean		4.19	.158
		95% Confidence Interval for Mean	Lower Bound	3.86	
			Upper Bound	4.51	
	From 10 to less than 15 years	Mean		4.60	.163
		95% Confidence Interval for Mean	Lower Bound	4.23	
			Upper Bound	4.97	
	From 15 to less than 20 years	Mean		4.50	.230
		95% Confidence Interval for Mean	Lower Bound	3.99	
			Upper Bound	5.01	
	From 20 years and over	Mean		4.67	.333
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	6.10	
SAFIU collects information about suspicious and fictitious companies and institutions	Less than 5 years	Mean		4.24	.291
		95% Confidence	Lower Bound	3.62	

APPENDIX D
Findings of the Kruskal-Wallis Test

companies and institutions.		Interval for Mean	Upper Bound	4.85	
	From 5 to less than 10 years	Mean		4.19	.130
		95% Confidence Interval for Mean	Lower Bound	3.92	
			Upper Bound	4.45	
	From 10 to less than 15 years	Mean		3.70	.260
		95% Confidence Interval for Mean	Lower Bound	3.11	
			Upper Bound	4.29	
	From 15 to less than 20 years	Mean		4.25	.218
		95% Confidence Interval for Mean	Lower Bound	3.77	
			Upper Bound	4.73	
	From 20 years and over	Mean		3.67	.333
		95% Confidence Interval for Mean	Lower Bound	2.23	
			Upper Bound	5.10	
SAFIU provides training programs to financial and nonfinancial institutions to understand money laundering and terrorism financing rules and regulations.	Less than 5 years	Mean		3.76	.250
		95% Confidence Interval for Mean	Lower Bound	3.23	
			Upper Bound	4.30	
	From 5 to less than 10 years	Mean		4.06	.185
		95% Confidence Interval for Mean	Lower Bound	3.69	
			Upper Bound	4.44	
	From 10 to less than 15 years	Mean		4.60	.163
		95% Confidence Interval for Mean	Lower Bound	4.23	
			Upper Bound	4.97	
	From 15 to less than 20 years	Mean		4.17	.241
		95% Confidence Interval for Mean	Lower Bound	3.64	
			Upper Bound	4.70	
SAFIU exchanged information with other FIUs prior to joining Egmont Group.	Less than 5 years	Mean		3.47	.311
		95% Confidence Interval for Mean	Lower Bound	2.81	
			Upper Bound	4.13	
	From 5 to less than 10 years	Mean		4.03	.165
		95% Confidence Interval for Mean	Lower Bound	3.69	
			Upper Bound	4.37	
	From 10 to less than 15 years	Mean		4.90	.100
		95% Confidence Interval for Mean	Lower Bound	4.67	
			Upper Bound	5.13	
	From 15 to less than 20 years	Mean		4.58	.336
		95% Confidence Interval for Mean	Lower Bound	3.84	
			Upper Bound	5.32	
SAFIU should operate their offices in major cities.	Less than 5 years	Mean		4.24	.106
		95% Confidence Interval for Mean	Lower Bound	4.01	
			Upper Bound	4.46	
	From 5 to less than 10 years	Mean		4.38	.087
		95% Confidence Interval for Mean	Lower Bound	4.20	
			Upper Bound	4.55	
	From 10 to less than	Mean		4.80	.133

	15 years	95% Confidence Interval for Mean	Lower Bound	4.50	
			Upper Bound	5.10	
	From 15 to less than 20 years	Mean		4.83	.112
		95% Confidence Interval for Mean	Lower Bound	4.59	
			Upper Bound	5.08	
SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money laundering and terrorism financing.	Less than 5 years	Mean		4.24	.106
		95% Confidence Interval for Mean	Lower Bound	4.01	
			Upper Bound	4.46	
	From 5 to less than 10 years	Mean		4.56	.089
		95% Confidence Interval for Mean	Lower Bound	4.38	
			Upper Bound	4.74	
	From 10 to less than 15 years	Mean		4.90	.100
		95% Confidence Interval for Mean	Lower Bound	4.67	
			Upper Bound	5.13	
	From 15 to less than 20 years	Mean		4.83	.112
		95% Confidence Interval for Mean	Lower Bound	4.59	
			Upper Bound	5.08	

Number of training courses in the area of work

	Number of training courses in the area of work			Statistic	Std. Error
SAFIU is authorised to request additional information on money laundering and terrorist financing STRs from financial and non-financial institutions either directly or through anothet authority.	None	Mean		4.20	.200
		95% Confidence Interval for Mean	Lower Bound	3.64	
			Upper Bound	4.76	
	One training course	Mean		4.72	.109
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.95	
	Two training courses	Mean		4.67	.142
		95% Confidence Interval for Mean	Lower Bound	4.35	
			Upper Bound	4.98	
	Three training courses	Mean		4.95	.048
		95% Confidence Interval for Mean	Lower Bound	4.85	
			Upper Bound	5.05	
SAFIU receives money laundering and terrorism finance STRs through various channels.	None	Mean		4.20	.200
		95% Confidence Interval for Mean	Lower Bound	3.64	
			Upper Bound	4.76	
	One training course	Mean		4.78	.101
		95% Confidence Interval for Mean	Lower Bound	4.57	
			Upper Bound	4.99	
	Two training courses	Mean		4.92	.083
		95% Confidence Interval for Mean	Lower Bound	4.73	
			Upper Bound	5.10	
SAFIU has standardised STR froms that capture all the required	None	Mean		3.40	.245
		95% Confidence	Lower Bound	2.72	

APPENDIX D
Findings of the Kruskal-Wallis Test

information.		Interval for Mean	Upper Bound	4.08	
	One training course	Mean		3.78	.207
		95% Confidence Interval for Mean	Lower Bound	3.34	
			Upper Bound	4.21	
	Two training courses	Mean		3.83	.271
		95% Confidence Interval for Mean	Lower Bound	3.24	
			Upper Bound	4.43	
	Three training courses	Mean		4.52	.164
		95% Confidence Interval for Mean	Lower Bound	4.18	
			Upper Bound	4.87	
	Four training courses and more	Mean		4.72	.109
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.95	
SAFIU receives and reviews STRs that are not related to money laundering and terrorism finance.	None	Mean		3.60	.400
		95% Confidence Interval for Mean	Lower Bound	2.49	
			Upper Bound	4.71	
	One training course	Mean		2.78	.250
		95% Confidence Interval for Mean	Lower Bound	2.25	
			Upper Bound	3.31	
	Two training courses	Mean		2.92	.358
		95% Confidence Interval for Mean	Lower Bound	2.13	
			Upper Bound	3.70	
	Three training courses	Mean		3.10	.194
		95% Confidence Interval for Mean	Lower Bound	2.69	
			Upper Bound	3.50	
	Four training courses and more	Mean		2.94	.189
		95% Confidence Interval for Mean	Lower Bound	2.55	
			Upper Bound	3.34	
SAFIU ensures all STRs received are validated for completeness.	None	Mean		3.80	.200
		95% Confidence Interval for Mean	Lower Bound	3.24	
			Upper Bound	4.36	
	One training course	Mean		4.17	.121
		95% Confidence Interval for Mean	Lower Bound	3.91	
			Upper Bound	4.42	
	Two training courses	Mean		4.50	.151
		95% Confidence Interval for Mean	Lower Bound	4.17	
			Upper Bound	4.83	
	Three training courses	Mean		4.33	.126
		95% Confidence Interval for Mean	Lower Bound	4.07	
			Upper Bound	4.60	
	Four training courses and more	Mean		4.56	.121
		95% Confidence Interval for Mean	Lower Bound	4.30	
			Upper Bound	4.81	

STRs are analysed according to the suspicious nature of money laundering and terrorism financing.	Two training courses	Mean		4.83	.112
		95% Confidence Interval for Mean	Lower Bound	4.59	
			Upper Bound	5.08	

APPENDIX D
Findings of the Kruskal-Wallis Test

SAFIU has supervisors who are knowledgeable in analysing STRs.	None	Mean		4.80	.200
		95% Confidence Interval for Mean	Lower Bound	4.24	
			Upper Bound	5.36	
	One training course	Mean		4.72	.109
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.95	
	Two training courses	Mean		4.92	.083
		95% Confidence Interval for Mean	Lower Bound	4.73	
			Upper Bound	5.10	
	Three training courses	Mean		4.90	.066
		95% Confidence Interval for Mean	Lower Bound	4.77	
			Upper Bound	5.04	
SAFIU recruits qualified and experienced personnel who possess the required skills in financial analysis.	None	Mean		4.00	.316
		95% Confidence Interval for Mean	Lower Bound	3.12	
			Upper Bound	4.88	
	One training course	Mean		4.17	.167
		95% Confidence Interval for Mean	Lower Bound	3.82	
			Upper Bound	4.52	
	Two training courses	Mean		3.92	.193
		95% Confidence Interval for Mean	Lower Bound	3.49	
			Upper Bound	4.34	
	Three training courses	Mean		4.19	.148
		95% Confidence Interval for Mean	Lower Bound	3.88	
			Upper Bound	4.50	
	Four training courses and more	Mean		4.56	.121
		95% Confidence Interval for Mean	Lower Bound	4.30	
			Upper Bound	4.81	

SAFIU staff members are informed about the sources of money laundering and the terrorism finance.	None	Mean		3.80	.200
		95% Confidence Interval for Mean	Lower Bound	3.24	
			Upper Bound	4.36	
	One training course	Mean		4.11	.179
		95% Confidence Interval for Mean	Lower Bound	3.73	
			Upper Bound	4.49	
	Two training courses	Mean		4.08	.229
		95% Confidence Interval for Mean	Lower Bound	3.58	
			Upper Bound	4.59	
	Three training courses	Mean		4.33	.126
		95% Confidence Interval for Mean	Lower Bound	4.07	
			Upper Bound	4.60	
	Four training courses and more	Mean		4.72	.109
		95% Confidence Interval for Mean	Lower Bound	4.49	
			Upper Bound	4.95	

SAFIU under SAMA's supervision imposes control over financial institutions to ensure compliance of its policy relating	One training course	Mean		4.39	.118
		95% Confidence Interval for Mean	Lower Bound	4.14	
			Upper Bound	4.64	

APPENDIX D
Findings of the Kruskal-Wallis Test

compliance of its policy relating to combating money laundering and the terrorism finance.	Two training courses	Mean		4.25	.131
		95% Confidence Interval for Mean	Lower Bound	3.96	
			Upper Bound	4.54	
	Three training courses	Mean		4.57	.111
		95% Confidence Interval for Mean	Lower Bound	4.34	
			Upper Bound	4.80	
	Four training courses and more	Mean		4.17	.090
		95% Confidence Interval for Mean	Lower Bound	3.98	
			Upper Bound	4.36	
SAFIU disseminates latest information regarding money laundering and terrorism finance received to fellow government agencies.	None	Mean		3.40	.600
		95% Confidence Interval for Mean	Lower Bound	1.73	
			Upper Bound	5.07	
	One training course	Mean		3.94	.127
		95% Confidence Interval for Mean	Lower Bound	3.68	
			Upper Bound	4.21	
	Two training courses	Mean		3.33	.225
		95% Confidence Interval for Mean	Lower Bound	2.84	
			Upper Bound	3.83	
	Three training courses	Mean		4.00	.138
		95% Confidence Interval for Mean	Lower Bound	3.71	
			Upper Bound	4.29	
	Four training courses and more	Mean		4.06	.056
		95% Confidence Interval for Mean	Lower Bound	3.94	
			Upper Bound	4.17	
SAFIU regularly releases periodic reports which include statistics, typologies and trends as well as information regarding its activities.	None	Mean		4.80	.200
		95% Confidence Interval for Mean	Lower Bound	4.24	
			Upper Bound	5.36	
	One training course	Mean		4.22	.236
		95% Confidence Interval for Mean	Lower Bound	3.72	
			Upper Bound	4.72	
	Two training courses	Mean		4.00	.369
		95% Confidence Interval for Mean	Lower Bound	3.19	
			Upper Bound	4.81	
	Three training courses	Mean		4.76	.136
		95% Confidence Interval for Mean	Lower Bound	4.48	
			Upper Bound	5.05	
The Saudi Permanent committee on Combatig money laundering (PCCML) supports SAFIU objectives.	None	Mean		3.60	.678
		95% Confidence Interval for Mean	Lower Bound	1.72	
			Upper Bound	5.48	
	One training course	Mean		3.50	.345
		95% Confidence Interval for Mean	Lower Bound	2.77	
			Upper Bound	4.23	
	Two training courses	Mean		3.00	.477
		95% Confidence Interval for Mean	Lower Bound	1.95	
			Upper Bound	4.05	
	Three training courses	Mean		4.14	.232
		95% Confidence	Lower Bound	3.66	

APPENDIX D
Findings of the Kruskal-Wallis Test

		Interval for Mean	Upper Bound	4.63	
	Four training courses and more	Mean		4.67	.114
		95% Confidence Interval for Mean	Lower Bound	4.43	
			Upper Bound	4.91	
Financial institutions have advanced awareness and knowledge of the danger of money laundering and the terrorism financing.	None	Mean		4.20	.800
		95% Confidence Interval for Mean	Lower Bound	1.98	
			Upper Bound	6.42	
	One training course	Mean		3.56	.381
		95% Confidence Interval for Mean	Lower Bound	2.75	
			Upper Bound	4.36	
	Two training courses	Mean		3.83	.386
		95% Confidence Interval for Mean	Lower Bound	2.98	
			Upper Bound	4.68	
	Three training courses	Mean		4.14	.303
		95% Confidence Interval for Mean	Lower Bound	3.51	
			Upper Bound	4.77	
	Four training courses and more	Mean		4.94	.056
		95% Confidence Interval for Mean	Lower Bound	4.83	
			Upper Bound	5.06	
Busineses have awareness and knowledge of the danger of money laundering and the terrorism financing.	None	Mean		4.20	.800
		95% Confidence Interval for Mean	Lower Bound	1.98	
			Upper Bound	6.42	
	One training course	Mean		3.28	.449
		95% Confidence Interval for Mean	Lower Bound	2.33	
			Upper Bound	4.22	
	Two training courses	Mean		3.17	.562
		95% Confidence Interval for Mean	Lower Bound	1.93	
			Upper Bound	4.40	
	Three training courses	Mean		4.33	.311
		95% Confidence Interval for Mean	Lower Bound	3.68	
			Upper Bound	4.98	
	Four training courses and more	Mean		4.94	.056
		95% Confidence Interval for Mean	Lower Bound	4.83	
			Upper Bound	5.06	
SAFIU cooperates with authorities in investigating cases related to money laundering and terrorism finance.	None	Mean		4.80	.200
		95% Confidence Interval for Mean	Lower Bound	4.24	
			Upper Bound	5.36	
	One training course	Mean		4.44	.185
		95% Confidence Interval for Mean	Lower Bound	4.05	
			Upper Bound	4.83	
	Two training courses	Mean		4.42	.193
		95% Confidence Interval for Mean	Lower Bound	3.99	
			Upper Bound	4.84	
	Three training courses	Mean		4.76	.136
		95% Confidence Interval for Mean	Lower Bound	4.48	
			Upper Bound	5.05	

APPENDIX D
Findings of the Kruskal-Wallis Test

SAFIU exhchanges information regarding complex and unusual transactions with government and non-government organisations.	None	Mean		4.40	.600
		95% Confidence Interval for Mean	Lower Bound	2.73	
			Upper Bound	6.07	
	One training course	Mean		4.28	.289
		95% Confidence Interval for Mean	Lower Bound	3.67	
			Upper Bound	4.89	
	Two training courses	Mean		3.83	.441
		95% Confidence Interval for Mean	Lower Bound	2.86	
			Upper Bound	4.80	
	Three training courses	Mean		4.76	.136
		95% Confidence Interval for Mean	Lower Bound	4.48	
			Upper Bound	5.05	
SAFIU provides training programs to fellow government agencies that educate on combating money laundering and terrorism financing.	None	Mean		3.80	.200
		95% Confidence Interval for Mean	Lower Bound	3.24	
			Upper Bound	4.36	
	One training course	Mean		4.22	.173
		95% Confidence Interval for Mean	Lower Bound	3.86	
			Upper Bound	4.59	
	Two training courses	Mean		4.00	.174
		95% Confidence Interval for Mean	Lower Bound	3.62	
			Upper Bound	4.38	
	Three training courses	Mean		4.57	.130
		95% Confidence Interval for Mean	Lower Bound	4.30	
			Upper Bound	4.84	
	Four training courses and more	Mean		4.61	.118
		95% Confidence Interval for Mean	Lower Bound	4.36	
			Upper Bound	4.86	

SAFIU exchanged information with other FIUs prior to joining Egmont Group.	None	Mean		2.80	.490
		95% Confidence Interval for Mean	Lower Bound	1.44	
			Upper Bound	4.16	
	One training course	Mean		3.72	.278
		95% Confidence Interval for Mean	Lower Bound	3.14	
			Upper Bound	4.31	
	Two training courses	Mean		3.83	.322
		95% Confidence Interval for Mean	Lower Bound	3.13	
			Upper Bound	4.54	
	Three training courses	Mean		4.33	.211
		95% Confidence Interval for Mean	Lower Bound	3.89	
			Upper Bound	4.77	
	Four training courses and more	Mean		4.94	.056
		95% Confidence Interval for Mean	Lower Bound	4.83	
			Upper Bound	5.06	

SAFIU provides guidance to businesses for reporting and monitoring suspicious transactions related to money	One training course	Mean		4.39	.118
		95% Confidence Interval for Mean	Lower Bound	4.14	
			Upper Bound	4.64	

APPENDIX D
Findings of the Kruskal-Wallis Test

transactions related to money laundering and terrorism financing.	Two training courses	Mean		4.50	.151
		95% Confidence Interval for Mean	Lower Bound	4.17	
			Upper Bound	4.83	
	Three training courses	Mean		4.71	.101
		95% Confidence Interval for Mean	Lower Bound	4.50	
			Upper Bound	4.92	
	Four training courses and more	Mean		4.89	.076
		95% Confidence Interval for Mean	Lower Bound	4.73	
			Upper Bound	5.05	