UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Economic and Management Sciences

The Role of Internal Audit in the Independent Review of Anti-Money Laundering Compliance in South Africa

by

Thapelo Modisagae

Student Number

22020684

Submitted in partial fulfilment of the requirements for the degree

MPhil in Fraud Risk Management

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

Department of Auditing

at the

UNIVERSITY OF PRETORIA

Study Leader:

Mr Danie Du Plessis

October 2013

ACKNOWLEDGEMENTS

First and foremost, I would like to thank GOD Almighty, the author and the finisher of my faith who provides the source of all knowledge and inspiration. Without Him, I would not have had the perseverance and ability to complete this research.

I would like to express my sincere gratitude and acknowledgment for the support and help of my study leader Mr Danie Du Plessis who has provided an invaluable contribution and unwavering guidance throughout the course of this work. Your meticulous comments were an enormous help to me and your views on money laundering were highly illuminating.

Finally, I would like to dedicate this research to my family:

To my wife, Mrs Olebogeng Modisagae, I owe my deepest gratitude to you. Thanks for your encouragement, quiet patience and for your understanding when I spend many hours typing this research. Your unconditional love sustained me throughout.

To my parents, Mr David Modisagae, and Mrs Abigail Modisagae, thank you for instilling in me a firm determination to pursue education. The sacrifices you made throughout my years have been simply ineffable.

To my siblings, I know you always look up to me in some small way I hope I have inspired you.

PERSONAL DECLARATION

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Faculty of Economic and Management Sciences

Declaration Regarding Plagiarism

The Department of Auditing emphasises integrity and ethical behaviour with regard to the preparation of all written assignments.

Although the lecturer will provide you with information regarding reference techniques, as well as ways to avoid plagiarism, you also have a responsibility to fulfil in this regard. Should you at any time feel unsure about the requirements, you must consult the lecturer concerned before submitting an assignment.

You are guilty of plagiarism when you extract information from a book, article, web page or any other information source without acknowledging the source and pretend that it is your own work. This does not only apply to cases where you quote the source directly, but also when you present someone else's work in a somewhat amended (paraphrased) format or when you use someone else's arguments or ideas without the necessary acknowledgement. You are also guilty of plagiarism if you copy and paste information directly from an electronic source (e.g., a web site, e-mail message, electronic journal article, or CD-ROM) without paraphrasing it or placing it in quotation marks, even if you acknowledge the source.

You are not allowed to submit another student's previous work as your own. You are furthermore not allowed to let anyone copy or use your work with the intention of presenting it as his/her own.

Students who are guilty of plagiarism will forfeit all credits for the work concerned. In addition, the matter will be referred to the Committee for Discipline (Students) for a

ruling. Plagiarism is considered a serious violation of the University's regulations and may lead to your suspension from the University. The University's policy regarding plagiarism is available on the Internet at *http://www.library.up.ac.za/plagiarism/index.htm*.

For the period that you are a student at the Department of Accounting, the following declaration must accompany **all** written work that is submitted for evaluation. No written work will be accepted unless the declaration has been completed and is included in the particular assignment.

I Thapelo Modisagae, Student No. 22020684

Declare the following:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. I declare that this assignment is my own, original work. Where someone else's work was used (whether from a printed source, the Internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.

ABSTRACT

The dilemma of money laundering is an undeniable problem faced by many institutions all over the world. Due to its prevalence, the need for organisations to deal with the problem has become a global priority, regardless of the size of the financial institutions. Despite the compliance AML efforts undertaken by various institutions, AML compliance appears to be a daunting challenge, the question posed by this research is whether there is a need for independent anti-money laundering (AML) compliance reviews, given the invasive nature of money laundering in financial institutions. Secondly, the research addresses the question of who is well positioned to perform the independent AML compliance reviews. In addressing the second question, the research will discuss why internal audit is an invaluable resource in terms of risk management processes and the reasons why they are an integral part of the AML solution.

Key words:

Anti-money laundering compliance
Anti-money laundering risk-based approach
AML compliance reviews
Compliance risk
Financial institutions
FICA
Internal auditing
Independent AML reviews
Money laundering

TABLE OF CONTENTS

GLOSSARY OF TERMS

Accountable institutions

An accountable institution is an entity as referred to in the Schedule 1 list of the Financial Intelligence Centre Act (As Amended), No. 38 of 2001 (FICA) (South Africa) (FIC, 2010: 30).

Anti-money laundering compliance

This refers to measures taken by financial institutions to address money laundering and ensure compliance to laws and regulations (Mills, 2008: 18).

Anti-money laundering compliance reviews

Anti-money laundering (AML) compliance reviews test a financial institution's adherence to its compliance programme and to its regulatory responsibilities (Husisian, 2010: 20). For the purposes of the research, the word "review" is used synonymously with the words "audit" and "test" (i.e. anti-money laundering compliance audit/ review/ tests). All these words are used interchangeably when making reference to AML compliance programmes.

Anti-money laundering/combating the financing of terrorism

Post-September 2001, money laundering control measures have become closely linked with the measures to prevent the financing of terrorism. The relationship has grown so close that the control regime is generally referred anti-money laundering/combating the financing of terrorism (AML/CFT) (Johnson, 2008: 7).

Asia/Pacific Group on Money Laundering

This group is an autonomous regional Financial Action Task Force (FATF) body. Members work together to combat money laundering and the financing of terrorism through the AML/CFT standards (Johnson, 2008: 9)

Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision is an international forum facilitating regular cooperation regarding banking regulation. The main aim of the Basel Committee is to enhance the understanding of key supervisory issues and improve the quality of banking supervision globally (FATF, 2007: 30).

Caribbean Financial Action Task Force

The Caribbean FATF is a regional body formed in 1990 and represents 30 countries in the Caribbean Basin (Johnson, 2008: 9).

Consulting services

Consulting is an "advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organisation's governance, risk management, and control processes without the internal auditor assuming management responsibility." Other examples of these include counselling, advising, facilitation and training (IIA, 2012c: 20).

Chief audit executive

This is the employee who is responsible for managing the internal audit activity in accordance with the internal audit charter, code of ethics and standards (IIA, 2012c: 19).

Chief Risk/Compliance Officer

The employee responsible for providing education, methodologies and techniques that line and staff functions need to adhere to as part of their risk management and compliance responsibilities. The officer is also responsible for coordinating activities with line and staff leaders, general counselling and monitoring the reporting process (Steinberg, 2005: 21).

Compliance

In the context of financial services, compliance is defined as the function of identifying the relevant legislative, regulatory and best practice requirements and implementing the necessary systems and controls to ensure adherence to laws and regulations (Mills, 2008: 18). Furthermore, it refers to compliance with policies, plans, procedures, laws, regulations, contracts and other regulatory requirements (IIA, 2012c: 19).

Customer due diligence

This is the process of identifying the customer and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source (FSA, 2007). It involves establishing the true identity of a customer, determining the source of their funds and determining their relationship with the financial institution (Risk Solutions Financial Services, 2007: 4).For the purposes of the research, the term "customer due diligence" or CDD is used synonymously with "Know your Customer" or KYC. These words are used interchangeably with one another when making reference to the process of identifying a customer before engaging in business.

Designated non-financial businesses and professions

Designated non-financial businesses and professions in terms of the FICA refers to attorneys (which includes notaries), trust service providers, (real) estate agents, casinos and public accountants who carry on the business of rendering investment advice or investment broking services (FATF, 2009b: 11).

Eastern and Southern African Anti-Money Laundering Group

A FATF regional body with 14 members that has been in operation since 1999. The group's objective is to combat money laundering through the implementation the Financial Action Task Force Forty Recommendations (FATF 40 Recommendations) (Johnson, 2008: 9).

Egmont Group

A group of Financial Intelligence Units worldwide whose responsibility it is to improve cooperation in the fight against money laundering and the financing of terrorism and to promote the implementation of domestic programmes (Egmont Group, 2004).

Financial Intelligence Centre Act (As Amended), No. 38 of 2001

This law is abbreviated to "FICA". The aim of FICA is to provide a legal framework for effective money laundering control in South Africa (FIC, 2011/2012: 6).

Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental organisation that sets standards, develops and promotes policies to combat money laundering and terrorist financing (FATF, 2007: 30).

Financial Action Task Force Recommendations

This refers to internationally endorsed standards for implementing effective AML/CFT measures released by the FATF in October 2003. The aim of the recommendations is to increase the transparency of the financial system and assist countries to take action against money launderers and terrorist financiers (FATF, 2010a: 2).

The financing of terrorism

The financing of terrorism refers to "the direct or indirect provision of financial or economic benefit to support terrorism or related activity or any person or group engaging in such activity" (IRBA, 2011: 5).

Financial institutions

Entities that provide a range of financial activities as defined in the glossary of the FATF Recommendations. The term is used to refer to

> any person or entity who conducts as a business one or more of the following activities:
>
> - acceptance of deposits and other repayable funds from the public
> - lending

- financial leasing
- the transfer of money or value
- issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)
- financial guarantees and commitments
- trading in, (a) money market instruments (cheques, bills, cheque deposits, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading
- participation in securities issues and the provision of financial services related to such issues
- individual and collective portfolio management
- safekeeping and administration of cash or liquid securities on behalf of other persons
- otherwise investing, administering or managing funds or money on behalf of other persons
- underwriting and placement of life insurance and other investment related insurance
- money and currency changing (FATF, 2012: 115).

Financial Intelligence Unit

The Financial Intelligence Unit is "a central, national agency responsible for receiving, analysing and disseminating to competent authorities, disclosures of financial information: *(i)concerning suspected proceeds of crime*, or *(ii) required by national legislation or regulation,* in order to counter money laundering" (Egmont Group, 2004: 4).

Financial services provider

Asset managers, linked investment service providers and financial services providers who collect premiums or receive and/or hold customers' funds (FATF, 2009b: 129).

The FATF of South America against Money Laundering

This is a regional body member formed in 2000 to combat money laundering and terrorist financing. The body consists of representatives of the governments of ten countries, namely Argentina, Bolivia, Brazil, Chile, Columbia, Ecuador, Mexico, Paraguay, Peru, and Uruguay (Johnson, 2008: 9).

Hawala

Hawala is an alternative remittance system focusing on informal fund transfers that involve trade between distant regions in which conventional banking instruments are either weak or absent (Zagaris, 2007: 157-158).

Internal audit independence

This refers to an internal audit that is performed responsibly and in an unbiased manner (IIA, 2012c: 21).

Independent AML review

Independent testing performed by a function and/or individuals who are not responsible for the execution and monitoring of a bank AML program (Beaumier, 2005/2006: 31).

Intergovernmental Action Group against Money Laundering in Africa

A FATF regional body member formed in 1999 to combat money laundering through the implementation the FATF 40 Recommendations (Johnson, 2008: 9).

Internal Auditing

Internal auditing is

> "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" (IIA, 2010).

Integration

This is the final stage of the money laundering process. If the layering process succeeds, integration schemes place the laundered proceeds back into the legitimate economy so that they appear to be part of legal business funds (Hopton, 2006: 2-3).

King III Report

This is the third report on corporate governance that was revised after the new Companies Act No. 71 of 2008 came into effect and in response to changes in international governance trends. The report was compiled by the King Committee with the help of the King subcommittees (Institute of Directors in Southern Africa, 2009: 4).

Layering

Layering is the second stage in the money laundering process. This involves separating criminal proceeds from their source by using complex layers of financial transactions with the intention of concealing the audit trail (Hopton, 2006: 2-3).

Middle East and North Africa Financial Action Task Force

A FATF regional body member formed in 2004 to foster cooperation on matters relating to money laundering and the financing terrorism (Johnson, 2008: 9).

Money laundering

Money laundering in general refers to “any act that obscures the illicit nature or the existence, location or application of proceeds of crime” (De Koker, 2012: Com 1-4).

New FATF Recommendations

These recommendations refer to international standards and guidelines for combating money laundering and the financing of terrorism. The standards are internationally endorsed as effective in implementing AML/CFT measures and were released by the FATF in February 2012. They set out a comprehensive and consistent framework of guidelines and standards which countries should implement in order to combat money laundering and terrorist financing (FATF, 2012: 7).

Ongoing monitoring

This requires the continual scrutiny of transactions throughout the course of the relationship between entities and individuals to ensure that the transactions are consistent with the service provider's knowledge of the customer, their business and risk profile (FSA, 2007).

Placement

This is the initial stage of money laundering. Criminally acquired money is directly or indirectly placed into a financial system (Hopton, 2006: 2-3).

Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures

FATF regional body member formed in 1997 with members mainly from central and Eastern Europe. The aim of the committee is to combat money laundering through AML/CFT systems, international standards and the FATF Forty Recommendations plus the Nine Special Recommendations (FATF 40 + 9 Recommendations) (Johnson, 2008: 9).

Supervisors/regulators

These are the designated authorities responsible for ensuring the compliance of financial institutions with AML/CFT requirements (FATF, 2007: 41).

Uncovered Financial Institutions

The following financial institutions are collectively are referred to as "Uncovered Financial Institutions": "finance companies, leasing companies, collective investment scheme custodians, money lenders other than banks, and securities custodians licensed under the Financial Advisory and Intermediary Services (South Africa) Act [that] are not listed as accountable institutions for the purpose of the Financial Intelligence Centre Act" (FATF, 2009b: 90).

Wolfsberg Group

The Wolfsberg Group is an association of eleven global banks which has the objective of developing financial services industry standards and related products particularly for KYC and AML/CFT policies (The Wolfsberg Group, 2011).

LIST OF ABBREVIATIONS

09/11	The terrorist attacks on America on 11 September 2011
AFU	Asset Forfeiture Unit of the National Prosecuting Authority
AML	Anti-money laundering
AML/CFT	Anti-money laundering/combating the financing of terrorism
APG	Asia/Pacific Group on Money Laundering
BASA	Banking Association of South Africa
BSA	Bank Secrecy Act (USA)
BSA/AML	The Bank Secrecy Act (USA) specifically when referred to as an anti-money laundering law
BSD	Bank Supervision Department
CAE	Chief audit executive
CCO	Chief compliance officer
CDD	Customer due diligence
CEO	Chief executive officer
CIS	Collective investment schemes
CRO	Chief risk officer
CISC Act	Collective Investment Schemes Act
CSA	Control self-assessment
DNFBP	Designated non-financial businesses and professions
EDD	Enhanced due diligence
ERM	Enterprise risk management
ESAAMLG	The Eastern and Southern African Anti-Money Laundering Group
EU	European Union
EXCON	Exchange Control Department (South Africa)
FAIS	Financial Advisory and Intermediary Services (South Africa)
FATF	Financial Action Task Force
FATF 40 Recommendations	Recommendations released by FATF October 2003
FATF 40 + 9 Recommendations	The FATF Forty Recommendations plus the Nine Special Recommendations released by FATF
FDIC	Federal Deposit Insurance Corporation (USA)
FFIEC	Federal Financial Institutions Examinations Council

FI	Financial institution
FIC	Financial Intelligence Centre (South Africa)
FICA	Financial Intelligence Centre Act (As Amended), No. 38 of 2001 (South Africa)
FIU	Financial Intelligence Unit
FSA	Financial Services Authority (UK) newly named FCA (Financial Conduct Authority after its formation 1 April 2013)
FSB	Financial Services Board
FSP	Financial services provider
G-7	Original group of seven countries participating in financial agreements
G-10	New group of counties participating in financial agreements, currently more than ten members exist
GAFISUD	The FATF of South America Against Money Laundering (Grupo de Acción Financiera de Sudamérica)
GIABA	Intergovernmental Action Group against Money Laundering In Africa
HM Treasury	Her Majesty's Treasury (UK)
IA	Internal audit
IFT	Informal fund transfer
IIA	Institute of Internal Auditors
IMF	International Monetary Fund
IRBA	Independent Regulatory Board for Auditors
JMLSG	Joint Money Laundering Steering Group (UK)
JSE	Johannesburg Stock Exchange
MENAFATF	Middle East and North Africa Financial Action Task Force
MLR	Money laundering Regulations
MLRO	Money laundering reporting officer
ML/TF	Money laundering and terrorist financing
MLTFC Regulations	Money Laundering and Terrorist Financing Control Regulations
MoU	Memorandum of understanding
New FATF	New FAFT Recommendations released in February 2012

Recommendations	
NASDAQ	National Association of Securities Dealers Automated Quotation (US based Stock Exchange)
NYSE	New York Stock Exchange
OCC	Officer of the Comptroller of Currency
PAAB	Public Accountants and Auditors' Board (South Africa)
PEP	Politically exposed persons
POCA	Prevention of Organised Crime Act, No. 121 of 1998 (South Africa)
POCDATARA Act	The Protection of Constitutional Democracy against Terrorism and Related Activities Act of 2004 (South Africa)
PRECCA	The Prevention and Combating of Corrupt Activities Act No. 12 of 2004 (South Africa)
PwC	PricewaterhouseCoopers
RBA	Risk-based audit
SAR	Suspicious activity report
SARB	South African Reserve Bank (Central Bank)
SARS	South African Revenue Services
SPE	Special purpose entity
TBML	Trade-based money laundering
TF	Terrorist financing
UN	United Nations
UP	University of Pretoria

CHAPTER 1

INTRODUCTION AND GENERAL ORIENTATION

1.1. Background and Rationale

1.1.1. Money Laundering the Global Concern

> "Money laundering and the financing of terrorism are financial crimes with economic effects. They can threaten the stability of a country's financial sector or its external stability more generally. Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse. Action to prevent and combat money laundering and the financing of terrorism thus responds not only to a moral imperative, but also to an economic need" (Zhu, 2012).

Money laundering is a momentous global threat. Jurisdictions flooded with illicit funds are extremely vulnerable to the breakdown of law, the corruption of public officials and to the destabilising of economies (US State Bureau for International Narcotics and Law Enforcement Affairs, 2012: 3).

Money laundering has thus become a major concern for law enforcement agencies worldwide and international crime syndicates relating to money laundering are becoming prominent in South Africa. Financial institutions such as life insurers, banks and investment houses have become prime targets for illegal activities (De Kock, Kruger, Roper, & Odendaal, 2002: 147).

From an African viewpoint, Moshi (2007: 9) points out that there are many challenges facing African countries regarding money laundering that require careful consideration. These obstacles range from the structure of national economies to reduced human and institutional capacity and the scarcity of resources.

Concerns have been raised by the international community about the integrity and stability of the financial system given the amount of money being laundered. Banks and other financial institutions may knowingly or unknowingly be used as intermediaries for the disposal of criminal proceeds (Johnson & Lim, 2002: 7). Johnson and Lim (2002: 8) argue that banks are central to money laundering activities because they provide three major advantages: convenience, accessibility and security.

Unger (2007: 29) highlights the crucial viewpoint that money laundering is largely a secretive phenomenon. It is a problem much larger than one could possibly imagine and remains, for the most part, in the dark and only brought to the light when detected. The exact number of launderers that operate over a given period of time, how much money they launder, which countries and sectors and which techniques are used is unknown and cannot be estimated with precision. Thus it is very difficult to measure the impact of money laundering.

Despite the challenges in quantifying the extent of money laundering, the amount of money laundered internationally is estimated to be roughly between US$1 and 3 trillion each year. Through western banking systems, drug traffickers are estimated to be dealing with US$1 trillion annually (Sinason, Pacini, & William, 2003: 11).

In 2004 it was estimated that every year AUS$4 billion are laundered through Australia, placing the country's financial institutions at risk of misuse (Garbutt, 2011: 31). Mulig and Murphy (2004: 22) claim that although it is difficult to measure the extent of money laundering, numerous attempts have been established to quantify the enormity of the problem. They estimated money laundering to be roughly US$500 billion a year in 2004.

In the early twenty-first century more than £200 million of crime-related funds passed though the financial institutions of the City of London (Kruger, 2008: 15). In 2011, criminals, particularly drug traffickers, may have laundered around US$1.6 trillion, the equivalent of 2,7 per cent of the global GDP in 2009, as reported by the United Nations (UN) Office on Drugs and Crime. This figure is consistent with the two to five per cent range previously established by the International Monetary Fund to estimate

the scale of money laundering (UNODC, 2011: 5-7). The above serves as an indication of how difficult it is to quantify the extent of money laundering.

Money laundering is very complex and at times not possible to measure accurately. Despite the vigorous international AML efforts, money laundering continues to increase yearly (Angel & Demitis, 2005: 271).

1.1.2. The Formation of International Bodies in Response to Money Laundering

The fight against money laundering has undergone two major transformations. The first transformation took place in the late 1980s and early 1990s. At the time, money laundering was viewed as a financial crime to be managed at national level. With the inception of the Financial Action Task Force (FATF), anti-money laundering (AML) was viewed as a global concern, especially in connection with drug trafficking. The second wave of transformation was after the events of 9/11. With this transition, money laundering became associated with terrorism (Helgesson & Morth, 2012: 2).

The global financial crisis in 2008 led to the modification of international financial architecture, in particular, the need for a regulatory framework that introduces greater transparency and accountability while minimising risks was addressed. Efforts to reinforce AML/CFT became an integral part of this process (FIC, 2011/2012: 10).

The official views on money laundering prevention measures embody three important principles: they deprive criminals of their illicit assets and expected revenue; they impose on criminals the need to launder their ill-gotten assets and thirdly, money laundering prevention efforts increase the probability of launderers being detected and convicted (Geiger & Wuensch, 2007: 92).

A key issue involved in AML is ensuring that critical information is made available to the right people, and that investigators and prosecutors are given adequate authority to convict criminals (Egmont Group, 2004: 1-2).

In support of global efforts, the Egmont Group (Egmont Group, 2004: 1-2) highlights that AML effectively requires knowledge of not only laws and regulations, investigation and analysis, but also of banking, finance, accounting and other related economic activities.

Jensen and Png (2011: 114) argue that if opportunities for money laundering are minimised, criminal activities will also be reduced as it will be much more difficult for criminals to use the proceeds unlawfully gained. Countries will benefit from a properly regulated financial sector, a functioning legal system and a law enforcement structure which forms the foundations of AML/CFT requirements.

In reaction to the epidemic, a number of governmental agencies have been formed as countries develop systems to deal with the problem of money laundering. These agencies are commonly known as the “financial intelligence units”. These units have played a vital role in money laundering programmes in the midst of the rapid exchange of information between financial institutions, law enforcement and various jurisdictions (Egmont Group, 2004: 1-2).

The focal point of the FIU before 9/11 was largely on the detection of suspicious transactions and reporting these. However, after the attacks, the scope of AML was rapidly expanded to cover the financing of terrorism and financial data made available to protect national security. The international mechanisms already in place were to enable the sharing of information between FIUs and related authorities and were further harnessed for this purpose (FIC, 2011/2012: 10).

In the same manner, the Egmont Group was formed. The Egmont Group is made up of national FIUs, specialised government agencies responsible for handling money laundering activities and suspicious activity reports (SARs). The Egmont Group provides a platform for discussing and improving the support of national AML programmes (Leong, 2007: 149).

The World Bank and the International Monetary Fund (IMF) have played a normative role in promoting an AML environment. By promoting financial sector reforms within individual countries, the role of the World Bank and the IMF in proactively facilitating

the fight against money laundering is well entrenched. They promote financial sector reform through their broad mandate, particularly in relation to good governance and the enforcement of prudent measures (Mugarura, 2011: 186).

The private sector also continues to set standards and shape the many expectations for AML programs. In November 2002, for example, the Wolfsberg Group of international financial institutions published its principles for Correspondent Banking as well as New York Clearing house “best practice” guidelines on correspondent banking which contributed positively towards many AML correspondent and compliance programmes (Beaumier & Shah, 2003: 14). The formation of the Wolfsberg Group was aimed at developing financial services industry standards. With the help of Transparency International the Wolfsberg Group set up global AML guidelines which were officially named the “Wolfsberg Anti-Money Laundering Principles” (Mohamed, 2002: 68).

Additionally, trade associations and self-regulating bodies, including, but not limited to, the American Bankers Associations, the Securities Industry Association, the Managed Funds Association and the National Association of Securities Dealers continue to issue guidance to the financial services industry (Beaumier & Shah, 2003: 14). The most noteworthy initiative is the FATF recommendations which focus on prevention, law enforcement and international cooperation (Goredema, 2007: xi).

The Basel Committee was established by the Central Bank Governors of the G-10 countries to put together broad supervisory standards and guidelines and further best practice recommendations. The IMF and World Bank have also joined the global anti-money laundering drive and contributed to FATF’s efforts in a number of areas (Leong, 2007: 149-150).

As a result of government concerns globally, laws were passed in countries such as the US to combat money laundering and terrorist financing. Such legislation embodied the recommendations from the FAFT. As a result, financial institutions in many countries have taken steps to implement appropriate policies and infrastructure to ensure compliance with AML requirements and practices. One crucial step was to implement the anti-money laundering and counter terrorist

financing (AML/CFT) programmes based on the FAFT recommendations (Khan, 2007: 46).

1.1.3. Global Frameworks to Combat Money Laundering

According to Axelrod and Ross (2012: 72), an AML programme consists of four main pillars: a system of internal controls to ensure ongoing compliance, independence testing for compliance, the designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance and a training programme appropriate for compliance personnel. The mere presence of these pillars without proper integration does not produce the best results.

Equally important is the reporting of suspicious and unusual transactions and the foundation of an effective preventative programme of AML/CFT (De Koker, 2002b: 147). The international community agrees that measures such as client identification, record keeping and the reporting of suspicious transactions should be used as an integral part of preventing and deterring money laundering (De Koker, 2012: Com 1-3).

The FATF (2012: 14-15,19), through the New FAFT Recommendations, advocates regular compliance from financial institutions by performing regular customer due diligence (CDD) checks, record keeping and reporting of suspicious transactions. The FATF recommendations also include the implementation of a risk-based approach in addressing money laundering. By and large this process includes recognising the existence of the risk(s), performing a risk assessment and developing strategies to manage and mitigate the identified risks (FATF, 2007: 2).

Although there is no unanimously accepted methodology that fully describes the nature and extent of a risk-based approach, the FATF (2007: 2) argues that an effective risk-based approach should at least identify and categorise money laundering risks and, in response to the risks identified, establish practical controls to ensure they are adequately mitigated. It is through an effective risk-based approach that financial institutions can exercise reasonable business judgement regarding their customers.

Nonetheless, Moshi (2007: 9) highlights that the FATF and other international standards do not appear realistic in terms of preventing and detecting money laundering in predominantly cash-based economies and countries. The issues relevant and prevalent in most African countries may call for an adapted solution that fits the continent.

Moshi (2007: 9) challenges the practice of labelling African countries as either compliant or non-compliant. He argues that it is unrealistic because it fails to take into consideration the challenges faced by the continent such as extreme poverty, under-resourced government agencies, the severe lack of skilled human capital, a dominant informal sector, the predominantly cash-based economies and the weak information and communication infrastructure.

1.2. Anti-Money Laundering Non-Compliance and Independent AML Reviews

The financial industry's responsibility to identify and limit money laundering is colossal. However, failure to do so carries significant risks including the operational, reputational and financial dangers associated. This may also result in regulatory penalties, forced operational and policy changes, frozen assets and the loss of revenue streams. The customer base may also be lost because of negative publicity (Risk Solutions Financial Services, 2010: 3).

There is generally an increased burden on banks to comply with additional laws and regulations emanating from the US Patriot Act of 2001. Accordingly, banks have had to increase their compliance staff, develop more sophisticated technology and devote additional resources to monitoring and complying with AML/CFT (Pasley, 2011: 42). The United States views independent auditing as one of the four pillars of an AML programme and advocates a system of compliance, controls, designated AML compliance officers and continuous AML training (Delston, 2007: 5).

In addition, the release of the *Bank Secrecy Act Anti-Money laundering Examination Manual* has ensured that the current spotlight on money laundering compliance

continues to shine (Beaumier, 2005/2006: 31). The manual was released in June 2005 by the Federal Financial Institutions Examinations Council's (FFIEC).

In December 2005, ABN AMRO, one of the world's largest banks, valued at US$830 billion, was fined US$80 million for violating state and anti-money laundering rules and regulations. The bank has over 3 000 branches and subsidiaries spread over 60 countries (Unger, 2007: 1-2). This indicates the prevalence of money laundering.

In terms of the AML, the US authorities found that ABN AMRO contravened three of the four AML compliance criteria. The bank failed to maintain an adequate system of internal control, to integrate publically available data regarding shell companies into its automated monitoring systems and to adequately report suspicious activities (Unger, 2007: 1-2).

US authorities and the Central bank of the Netherlands found, amongst other things, that ABN AMRO lacked an adequate system of risk management procedures, corporate governance, auditing and legal review methods. The bank failed to adequately report suspicious transactions and to perform proper investigations on enquiries referred to its New York branch. When dealing with "high risk" correspondence banking customers ABN AMRO also overstated its CDD level (Unger, 2007: 1-2).

Similarly, in a review performed by the UK Financial Services Authority (FSA), several weaknesses were identified with a number of banks. It claimed that these banks appeared unwilling to turn away from profitable relationships despite the unacceptable risks involved in handling the proceeds of criminal activities (Salih, 2011: 24).

Nearly a third of banks, including the private banking arms of some major banking groups, appeared willing to accept a high level of money laundering risks provided their current reputation and regulatory risk was acceptable. More than half of banking institutions failed to apply meaningful enhanced due diligence (EDD) methods in higher risk situations and one-third of the banks dismissed allegations of dealing with

customers without an adequate review and another third failed to spot politically exposed persons (Salih, 2011: 24).

Additionally, three quarters of the banks reviewed failed to take adequate measures to establish the source of funds to be used in the relationship and its legitimacy, while with other banks the review pointed out that the AML risk assessment frameworks were not robust enough to adequately address the actual risk posed. These are cases to demonstrate that AML compliance is a recurring concern. It is clear that not all banks are complying with the set AML programmes and the tolerance level for money laundering risk appears to be much higher than for the reputation and regulatory risk (Salih, 2011: 24).

Beaumier (2005/2006: 31) argues that the responsibility of ensuring that the bank AML programme is effective is a shared organisational responsibility among the board of directors, senior management, AML compliance officers, the operations department and other relevant parties. However, the success of the AML programme lies in internal auditing or with another independent third party mandated to perform independent tests on a bank's AML programme.

To comply with the current rules, laws and regulations, board members are seeking to understand enterprise risk management (ERM) in the context of compliance. Internal auditing provides an opportunity to align sustainable good governance, ERM and to obtain greater value from compliance service (Julien & Richards, 2008: 43-44).

According to Rossiter (2007: 34), internal auditing services are a critical part of the governance framework and must work with management, the board of directors and external auditors. Internal auditing is refining risk identification and assessment capabilities and enhancing risk-based auditing that is aligned to organisational priorities and provides assurance where it is most needed.

1.3. Anti-money Laundering Compliance and the Necessity for Independent Reviews

1.3.1. Anti-Money Laundering Compliance

Much has been written about chief compliance officers, chief risk officers and other persons with similar job titles. Since the American Sarbanes-Oxley Act of 2002, there has been a renewed focus on risk and compliance. Many questions were raised as to why compliance risk officers and chief compliance officers are needed and the role they should serve (Steinberg, 2005: 20).

Perhaps it is also prudent to consider the difference between a chief compliance officer and a chief risk officer. A chief compliance officer (CCO) is concerned with adherence to the laws and regulations to which a company is subject. For the purposes of the research, these particular laws and regulations referred to are the AML laws and regulations. The chief risk officer (CRO) has a broader focus and deals with the entire spectrum of risk operations and financial reporting as well as compliance with laws and regulations. The role of a CRO or CCO varies greatly from company to company but the key issue is that the role is clearly established in terms of good business practice. The officer must also meet certain requirements and interface effectively with other personnel in the organisation who have similar responsibilities (Steinberg, 2005: 20).

Every financial institution is charged with the responsibility to develop policies and procedures as a defence mechanism against money laundering. It is the duty of a financial institution to be aware of trends and adapt their method to address the scourge (Risk Solutions Financial Services, 2010: 2).

An established culture of AML compliance is central to the fight against money laundering is financial institutions. The key preventative measures highlighted by the FATF for financial institutions are to ensure CDD, record keeping and reporting of suspicious transactions (FATF, 2012: 16-19). Geister (2010: 2) argues that CDD is one of the best defences a financial institution can use to safeguard itself against money laundering. CDD is also commonly referred to as “Know your Customer” (KYC). Geister (2010: 2) gives the principles of CDD such as customer identification and EDD compliance that are integral to suspicious activity reporting.

Financial institutions can derive maximum value from the compliance efforts by recognising and highlighting the vital interrelationships between the Bank Secrecy Act (USA) (BSA) and AML compliance and between the overall customer relationship and the internal control structures across entity lines (Raghavan, 2006: 29). Gardner (2007: 335) highlights that the level of AML compliance within an organisation is a crucial indicator of having a high practice standard in an institution.

1.3.2. Views on Independent Anti-Money Laundering Reviews

Ongoing AML audits are key to ensuring consistent AML compliance and to help identify evolving risk management practices. AML compliance is mainly about processes rather than consistent results or documentation. The requirements are that financial institutions appoint a compliance officer, create internal AML policies and procedures, conduct ongoing training to support policies and procedures and test themselves with independent audit and reviews (Pallay, 2004: 37).

In Europe, independent audits do not feature in the European Union (EU) Third Directive. The Directive simply requires that financial institutions have appropriate policies and procedures for “internal controls”. The word “appropriate” may perhaps be construed to encompass independent reviews however the Directives do not explicitly state that independent reviews are a priority (Delston, 2007: 6).

The position in the UK is rather interesting. The principle of the annual review is contained in the FSA rules. The rules highlight that it is the money laundering reporting officer (MLRO), not the independent party, who must report at least once a year on the operation and effectiveness of an institution’s AML system and controls. The FSA rules places the onus on the institution itself to carry out regular assessments of systems and controls to ensure their compliance to set rules. Furthermore, given the FSA perspective, the Joint Money Laundering Steering Group (UK) (JMLSG) guidance contains no recommendations on independent reviews (Delston, 2007: 6).

In America, the US Patriot Act of 2001 requires that independent testing be performed by a separate function and individuals who are not responsible for the

execution and monitoring of a bank's AML programme. The emphasis is that independent reviews should be performed by an institution's internal audit department or alternatively by external assurance consultants. (Beaumier, 2005/2006: 31).

Khan (2007: 46) holds a similar opinion: independent testing by knowledgeable internal auditors is critical to ensuring AML/CTF programmes are comprehensive and fully aligned with regulatory requirements. Furthermore, the auditors must have in-depth knowledge of AML/CFT regulations, risks and controls. Khan (2007: 46) asserts that programme testing should be unified and well integrated. It must include a well-defined strategy and take the risks of the enterprise into account.

In Australia, the latest version (as of February 2007) of the proposed rules under the new AML stipulates that

> the financial institutions' risk based approach assessment and its risk awareness and employee due diligence programs should be subject to regular independent review: to assess their effectiveness, whether they comply with the Rules, whether they have been effectively implemented and whether the entity complies with the program (Delson, 2007: 5).

In Singapore, the AML regime requires banks to have an audit function that is adequately resourced and independent. The bank should be able to regularly assess the effectiveness of internal policies, procedures, controls and compliance with regulatory requirements (Delson, 2007: 5).

In the South African context, FICA does not specifically address the issue of an independent, internal audit function or identify independent AML reviews as a priority (De Koker, 2012: Com 6-6).

1.4. The Relevance of Internal Auditing in Anti-Money Laundering Compliance

The internal auditing profession has grown significantly in recent times. The increased awareness of the value of internal auditors, coupled with legislation in the public sector and the JSE prescriptions through the King III Report, have contributed immensely to the growth (IIA, 2008).

Internal auditors are registered members of the Institute of Internal Auditors. Local chapters exist in various countries where members can become affiliates of the Institution. The members of the Institution are governed by the framework known as the "International Standards for the Professional Practice of Internal Auditing". Compliance with the standards is essential to meeting the responsibilities internal auditors have and to the internal audit activity. One of the key objectives of the professional standards is to define principles that represent the practice of internal auditing (IIA, 2012a).

Internal audits are commonly performed by professionals with an in-depth understanding of the business culture, systems and processes. Internal auditing activities provide assurance to management and the auditing committee that internal controls are in place, are adequately designed and operating effectively to mitigate risks so that governance processes and organisational goals and objectives will be met (IIA, 2012a).

Nonetheless, Von Eck (2011: 6) draws attention to the view that, there is a general lack of understanding of what internal auditing is and as to the role of the internal auditing profession. Many organisations establish internal audit functions purely for the sake of compliance without understanding the value internal auditing can offer. It is critical that organisations understand the role of internal auditing as a key assurance of compliance to the board of directors through the audit committee.

Accordingly, the Institute of Internal Auditors (IIA) defines internal auditing as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its

objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes" (IIA, 2010).

Internal auditing has broadened in the past years by taking into consideration business complexities and consequence management. The argument is made that internal auditing can deliver greater value to the organisation by championing good governance, supporting Enterprise Risk Management (ERM) rollout, consolidating compliance processes and coordinating various monitoring functions (Julien & Richards, 2008: 43-44).

In the fight against money laundering, internal audit functions in banking and financial services industries must respond to new challenges and expectations. There is a need for auditing to provide greater value as a key component of an organisation's governance framework (Rossiter, 2007: 34). In this regard Harrington (2004: 65) affirms that internal auditing has an extensive role to the extent that the New York Stock Exchange (NYSE) now requires that listed companies maintain an internal auditing function to provide management and the audit committee with assurance of the company's risk management processes and system of internal control.

Veazie (2011: 9) shares a similar viewpoint stating that internal auditors are well positioned to evaluate business control systems and can be relied upon by management. Primarily this may be achieved by continuously reviewing the effectiveness of internal controls, the efficiency of operations, the accuracy of financial records and compliance to policies, laws and regulations.

Other arguments raised explain that internal auditing cannot perform compliance monitoring however it is in the position to provide assurance on the compliance process for a specified period. Compliance monitoring can only be effective if the implementation is continuous and internal audit reviews of the compliance function are completed annually to provide an expert opinion on whether or not the compliance is functioning properly and as intended (Terblanché, van der Merwe, & Schlebusch, 2008).

Therefore Sinason et al. (2003: 11) point out that generally an internal audit can only identify terrorist financing once it is at the stage where the organisation or individual has opened a bank account and has been directly involved in a financial transaction. This illustrates that the process of internal auditing is reactive in nature.

However Sinason et al. (2003: 11) reiterate that internal auditors are well positioned to detect suspicious transactions, particularly those involving money laundering in customer accounts. The requirements of the IIA Practice Advisory 1210.A2-1 indicate that the detection of fraud consists of identifying indicators of fraud sufficient to warrant an investigation and internal auditors are required to be aware of indicators of money laundering as a type of fraud.

1.5. The Purpose of the Research Report

The purpose of this research is to analyse the role that independent reviews and internal auditing can play in AML compliance reviews. Through this analysis, money laundering was revealed to be much more complex than anticipated and the important role that internal auditing can play in the independent review of AML programmes became apparent.

In this regard, the AML pillars, through the FATF New Recommendations (2012: 14-19), require onerous responsibilities and regular compliance of financial institutions which includes performing regular CDD checks, record keeping and reporting of suspicious transactions. The research demonstrates how an integrated approach including independent AML reviews performed by internal auditing can be the foundation for ensuring AML compliance.

1.5.1. Research Problem and Objectives

Kumar (2011: 44) highlights that in general any question, assumption or assertion can be challenged and become a research problem. However, it is important to note that not all problems can be transformed into research problems and they can prove to be difficult to study. The research problem serves as a foundation for the research study. It is important that the problem can be scrutinised in terms of the study.

In the last decade there has been an enormous drive to secure AML compliance in all major financial centres worldwide. The impact on the financial sector globally cannot be underestimated. Banks and other financial service providers find themselves in a position in which they are obliged to take responsibility for screening clients according to certain risk factors (Pieth & Aiolfi, 2002: 6). Likewise, in South Africa a number of laws have been enacted that target money laundering. The most crucial is the legislation by the FIC which created an administrative framework for money laundering control (De Koker, 2002b: 1).

The New FATF Recommendations point out that one of the measures which financial institutions can use to combat the problem is to have programmes against money laundering and terrorist financing. These programmes should at least include an independent auditing function to test the AML systems (FATF, 2012: 78). The US Patriot Act requires that independent testing be performed by a function and individuals who are not responsible for the execution and monitoring of a bank's AML programme (Beaumier, 2005/2006: 31).

Other equally strong viewpoints raised are that individuals performing independent reviews must be adequately qualified to execute them. In addition to basic auditing skills, independent auditors must have knowledge of the legal and regulatory requirements, a good understanding of the institution's customer base, as well as its products and services. Besides these requirements individuals performing the reviews must have technology skills and a good grasp of how AML software programs work (Beaumier, 2005/2006: 31).

Khan (2007: 46), who shares a similar viewpoint with Beaumier, maintains that audit teams need to understand an organisation's products, delivery channels, structure, infrastructure, type of clients including their geographical locations and the relevant policies, procedures and controls for mitigating the risks of money laundering and terrorist financing. As part of the auditing strategy, auditors need to list all regulatory requirements (in the country which the entity does business/operates), understand and define components and develop a risk profile for which an appropriate audit programme can be developed.

Kumar (2011: 50) points out that a primary (main) objective and sub-objectives (secondary objectives) should be established. The primary objective is the overall statement of the thrust of the study that the research seeks to understand, while the sub-objectives look at specific aspects of the topic that the research seeks to investigate.

The primary research objective is to investigate and address the following:

- Whether there is a need for independent AML reviews to assess and provide assurance on AML compliance within financial institutions.

Additionally, the research sub-objectives will consider the following:

- defining and understanding AML compliance reviews
- why regular independent AML compliance reviews are critical to the fight against money laundering
- a review of the FAFT recommendations and other international guidelines on AML compliance and independent AML reviews
- the South African perspective on AML compliance and independent AML reviews
- a comparison of South Africa's AML system with other leading international systems
- although there is no clarity as to who should perform independent AML reviews in the relevant literature, the research will consider whether internal auditing is in a position to perform these reviews.

1.6. Research Approach

1.6.1. Research Methodology

The first question to address is what the research seeks to discover, that is, the research problem. Having decided on the research problem, the researcher considers how the answer(s) to the research problem will be found. This will be the research methodology (Kumar, 2011: 18).

The research methodology is used as a tool to analyse the research problem and involves a literature review. A literature review is a summary of knowledge on a

particular subject that helps identify and describe the specific research question. It identifies and organises the concepts from the relevant literature. A literature review should draw on and evaluate a range of sources including journal articles, books and web based resources et cetera (Rowley & Slack, 2004: 31).

There are four aspects to consider when planning a literature review and these are the genre of literature, the types of sources, the timeframe available for research and the extent to which the literature will be covered. The objective of the literature review will determine the choices made for each of these aspects (Marrelli, 2005: 40).

The literature review condenses and summarises the existing literature on a subject (Rowley & Slack, 2004: 32). One of the first aims when performing a literature review is to find out what has been done previously in the field. A review of work by experts and researchers on the available body of knowledge is undertaken to determine how they have investigated the research problem. In this way one learns how others have theorised on the issues, what they have discovered through empirical research and what instruments they have used and to what effect. The most recent, credible and relevant writers will become the focus of the review (Mouton, 2001: 87).

Hofstee (2009: 91) points out that a good literature review is one that is comprehensive, critical and contextualised. Hofstee (2009: 105) further states that critical reviews are characterised by careful evaluation and judgement and do not consist merely of calling attention to errors and flaws.

For the purposes of this research, the focal point of the review will be on the literature relating to AML compliance, independent AML reviews and the role of internal auditors in these matters.

1.6.2. Advantages and Disadvantages of a Literature Review

The purpose of a literature review is to demonstrate an awareness of what is happening in a particular field of study, to demonstrate the theoretical basis of the work proposed, to show how the research to be undertaken fits in with what has been done previously and lastly to clearly demonstrate that the significance of the work and how it may potentially lead to new knowledge (Hofstee, 2009: 91).

A review may not necessarily produce completely original research but may communicate new views or interpretations of what has already been written. While performing a literature review, Hofstee (2009: 121) advises that careful consideration should be made of the sources to be used, their accuracy, how they represent and classify the subject, their conclusions, the contributions of other scholars and possible researcher bias.

Given that context, Mouton (2001: 87) highlights the fact that a literature review has certain advantages that are vital to its success. Some of these advantages include ensuring that the research does not merely duplicate previous studies; discovering the most recent and authoritative theorising about the subject matter; evaluating the widely accepted empirical findings in a particular field of study; identifying available information that has been proved in terms of validity and reliability; and ascertaining the most widely accepted definitions of key concepts in the field.

Marrelli (2005: 43) also argues in this regard that literature reviews are versatile in that they can be conducted on almost any topic and can provide information at a basic or in-depth level. Other arguments raised are that literature reviews are relatively economical and efficient because a large amount of data can be collected quickly at minimal cost.

A literature review has a number of advantages; however, it is also not without disadvantages. Some literature reviews are limited to collecting information about events that happened in the past and usually within organisations other than the researcher's own workplace. As a result they cannot provide data about current actual behaviour. Another facet is that an effective literature review requires a high level of skill in identifying resources, analysing the sources to identify relevant information and writing a meaningful summary, and this can sometimes be a challenge (Marrelli, 2005: 43-44).

Students may not have access to certain information and unnecessary time and resources may be spent on searching for sources for the reviews. Moreover, literature reviews can sometimes be time consuming for the study leaders to correct and provide feedback, particularly for students who are inexperienced in this type of assessment (Chan, 2009)

1.7. Research Design and Process

A research design is a procedural plan adopted by the researcher to respond to the research questions in an objective, relevant and efficient manner. The rationale and justification for decisions made are given and these are supported by the critical review of the literature (Kumar, 2011: 94).

Hofstee (2009: 91,105) argues that a good literature review should be inclusive, critical, contextualised and rest on a solid theoretical base. It should provide a critical and factual overview of past research. A critical overview is characterised by careful evaluation and judgement.

Leedy and Ormrod (2001: 77) state that the key aspect of a successful literature review lies in the ability to carefully integrate the information, thoughts and ideas of experts and present it in a manner that is well thought-out and logical.

The research was constructed using key words. The initial key words were “money laundering”, “AML compliance”, “AML reviews”, “independent AML reviews”, ”compliance risk”, “AML risk-based approach”, “FICA” and “internal auditing”. This set of words was later expanded to include “financial institutions’ AML measurers” and “AML programmes”.

Gathering evidence and information for research purposes requires careful consideration of the author, their background as it reveals the purpose and perspective that influenced their work, their credentials and how adequately they cover the topic. The publisher, when the work was published, the proposition or theme of the work and the appropriateness of the methods and evidence is also examined (Hofstee, 2009: 105-6). The type of sources will be described below.

1.7.1. Academic Books

A search for academic books in the University of Pretoria (UP) library yielded works focussing mainly on the money laundering process and techniques, and on detection, prevention and deterrence methods.

A number of books were considered for the purposes of the research. When evaluating the books consideration was given to their relevance to the research topic., Books written by authoritative authors (ascertained by their biographical details, experience and field), published by reputable publishers involved in the discipline and up-to-date books (as indicated by the publication date) were given preference (Rowley & Slack, 2004: 33).

No academic books explicitly addressing internal auditing and money laundering were found.

1.7.2. The UP Catalogue

A catalogue search of the UP libraries was performed for books written in the field of study. A similar approach was used for articles in periodicals, conference proceedings, reports, dissertations, websites and journal articles with preference given to peer review journals.

1.7.3. Journal Articles

A consistent approach was used to search for journals. The initial search was conducted on the academic search engines such as EBSCOHOST, Proquest and Google Scholar. The academic search engines led to a number of academic journals that provided insight and were subsequently used. A further search was conducted on the various journal websites, with preference given to peer-reviewed articles and journals published by accredited bodies. Relevant articles were found in the Journal of Money Laundering Control, the Journal of Banking Regulations and the Journal of Financial Crime for example.

1.7.4. Articles in Periodical Publications

A number of articles were found in periodic magazines and other publications. The magazine publications in most cases focus on a particular field such as accounting, general compliance and AML compliance and the information was very useful in the

research. The articles published were written by experts in their particular field. Articles were found in the following journals: *The Institute of Internal Auditors*, *Bank Compliance* and *Compliance Week*.

1.7.5. Self-Regulatory Bodies and Institutions (Web Resources)

Websites of highly-rated and regulated international and local institutions were searched for all pertinent information pertaining to the research topic. The search included the websites of the International Monetary Fund (IMF), the Independent Regulatory Board for Auditors (IRBA), the Financial Intelligence Centre (FIC), the Financial Action Task Force (FATF), the Financial Services Board (FSB), the Asset Forfeiture Unit of the National Prosecuting Authority (AFU) and the Banking Association of South Africa (BASA). The websites of these institutions provided links to other websites that were useful for research purposes.

When evaluating the web-based resources careful consideration was made of the intended audience, the frequency of information updates and what the web resource developer's claim to expertise and authority is (Rowley & Slack, 2004: 33).

1.7.6. Original Sources Cited by Authors

References used by the authors and institutional bodies of books, articles and journals and were useful as they provided additional sources of information.

1.8. Limitations

When writing about methodology, Oliver (2004: 134) states that it is a good idea to discuss the limitations of the approach chosen and that it is a part of the critical, academic style of research which highlights both the advantages and limitations of the chosen research perspective. Hofstee (2009: 117) points out that all methods of research have limitations and brainstorming is one of the means to establish limitations.

The research scope is limited mainly to AML compliance in financial institutions. Financial institutions, as defined in the glossary of the FATF Recommendations,

include *inter alia* persons or entities whose operations include accepting deposits, providing loans and finance leasing, issuing and managing payment methods, issuing financial guarantees and commitments and investing and managing funds on behalf of a third party (FATF, 2003b: 16).

According to the FATF (2003b: i), money laundering methods have changed in response to the development of counter-measures. The escalation of money laundering has become a worldwide concern and multi-faceted predicament. This is partly due to the increase in sophisticated technique combinations used by money launderers.

In reaction to money laundering, numerous AML guidelines and recommendations have been developed. However, for the purposes of this research and in drawing conclusions and inferences, the guidelines from the FATF, the European Union (EU), the US Patriot Act and the UK money laundering regime are used as they are considered the leading practices. This research also makes the assumption that the US AML administration in this regard is the leading organisation, if not the best, in the world, because the US has had to combat money laundering for the sake of national security in recent times.

In an effort to understand and assess the South African AML regime, the country's compliance to FAFT standards will be considered. Gaps and deficiencies will be identified in relation to the FATF standards. South African guidelines and legislature will not be compared with other leading practices.

In response to money laundering, South Africa implemented the AML/CFT preventative measures through the Financial Intelligence Centre Act of 2001 (FICA), the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations) and the FICA exemptions (FATF, 2009b: 8). The research solely looks at financial institutions from a FICA viewpoint when reviewing the South African AML system. The research will not review every framework that pertains to financial services or financial institutions. The FICA is the governing legislature for the Republic of South Africa and thus becomes the basis of comparison.

The evaluation performed by the FATF on South Africa AML compliance was performed in 2008, prior to the release of the New FATF Recommendations in 2012. No evaluation has been performed by the FATF since 2008. Presently, improvement may be necessary in certain areas but the conclusions highlighted in the 2008 FATF evaluation are noteworthy and require careful consideration.

To draw conclusions and provide comparisons particularly on independent AML reviews, South Africa and global leading practices such as FATF, European Union, US, and the UK's Money laundering regime were reviewed. However it must be noted that the mere basis of comparison will be based on the various regimes' views on independent AML reviews in order to address the research problem. The purposes of the research will not be to review every AML measures implemented by the various regimes and perform direct comparisons.

Given the scope of the FAFT 40 Recommendations, it is not feasible to cover them all in detail in this research. For the purposes of the research and to highlight key areas the three preventative pillars of the AML/CFT will be the focus. The three pillars are customer due diligence (CDD), record keeping, and the monitoring and reporting of suspicious transactions.

The FATF Recommendation number 15 lays the premise for the research foundation. The FATF Recommendation 15 states that

> Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include: The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; an ongoing employee training programme; and an audit function to test the system (FATF, 2003b: 8).

Although the FATF Recommendations provide a number of best practice guidelines for combating money laundering, for the purposes of the research attention will be given to Recommendation 15 (FAFT Recommendations) and Recommendation 18

(New FAFT Recommendations) which are aligned with the research topic and provide the basis of the arguments to be raised.

In attempting to address the research topic, this work will consider whether or not there is a need for independent AML reviews and why internal audit is best positioned to provide the independent assurance. The research will argue from an internal auditing viewpoint. It should be noted that the research will not argue whether the legal profession or any other profession can or cannot perform an independent review.

It should be noted that there are very few South African academic publications and professional journals on money laundering compliance. The information was found in legislation documents including the FICA, and the South African Bank Act No. 94 of 1990.

Since the 9/11 terrorist attacks in the US, money laundering and the financing of terrorism has been linked. Money laundering may be used to finance acts of terrorism (Johnson, 2008: 7). Although inferences will be drawn on terrorist financing, the research will not look at the subject in-depth.

To ensure that the research is relevant and refers to the most recent practices, all work published prior to 2000 was excluded other than legislation. Thus the majority of sources reviewed and used were published between 2001 and 2013.

1.9. Chapter Outline

This section provides an outline of the chapters of this report.

1.9.1. Introduction and General Orientation

This chapter sets out the basis for the research conducted. This includes a background to the research, the problem statement, the research objectives, research methodology and an overview of the structure of the report.

1.9.2. Anti-Money Laundering Compliance and Anti-Money Laundering Compliance Reviews

The section lays the foundation of AML preventative measures, looking specifically at compliance efforts made by financial institutions. It provides a holistic view of local and international AML compliance administration and provides a basic overview of what AML compliance is and what it entails.

Elaborating further the chapter then focuses on the adoption of a risk-based approach and risk management processes for dealing with money laundering. It considers risk(s) recognition, performing risk assessments and developing strategies to manage and mitigate the risks identified. In addition, it highlights and explains what compliance reviews are, their key objectives and requirements and how they are performed.

1.9.3. The Necessity of Independent Anti-Money Laundering Reviews

The chapter addresses the need for independent AML reviews particularly with regard to AML compliance programmes. Emphasis is placed on independent reviews performed by individuals free of bias, whose role does not conflict with an internal or external party, and who possesses the necessary skills and qualifications to adequately provide a valuable opinion on whether AML programmes are operating effectively as intended and are adequately mitigating the risk of money laundering. This chapter argues that there is a need for independence to ensure an effective risk management process.

1.9.4. The Financial Action Task Force and Other International Anti-Money Laundering Guidelines

This chapter looks at the various AML measures developed by the FATF, EU, USA, and UK. An overview of money laundering as a global problem is given by considering the FATF countermeasures and recommendations and other leading practices. The purpose of this chapter is to review and outline AML best practice guidelines on an international scale and the possible impact of the guidelines implemented in various countries. A greater emphasis is placed on guidelines that focus on AML compliance and independent reviews.

1.9.5. Anti-Money Laundering in South Africa and Anti-Money Laundering Counter Measures

This section reviews the money laundering problem faced in South Africa with reference to the environment and markets in which it operates. The financial impact and implications of money laundering are discussed as well as the abuse of the formal and informal financial sectors. A holistic view of AML/CFT measures and the legal and regulatory frameworks currently in place is provided. In line with the research topic, the chapter provides an assessment of independent AML compliance reviews from a FICA viewpoint in the South African context.

1.9.6. Comparative Analysis of South African Measures and Global Guidelines

This chapter compares South African AML measures with leading international practices. Comparisons are made specifically between South Africa and the FATF, EU, USA and the UK regimes in terms of AML measures and their views on independent AML reviews.

An analysis of the measures in place and further recommendations as to how certain aspects of the South African administration could be strengthened are given. The section also looks at the degree of South African compliance in terms of the FATF 40 + 9 Recommendations as highlighted in the 2008 FATF evaluation report.

1.9.7. The Role of Internal Auditing in Independent Anti-Money Laundering Reviews

The chapter explains the role internal auditing can play in independent AML reviews. The role of internal auditing is highlighted including its core responsibilities, its mandate regarding risk management process and an advisor to management. The need and role of internal auditing is described according to the King III Report requirements. In addition, this chapter shows how the King III Report emphasises the importance of internal auditing for risk management assurance.

The section outlines the importance of internal auditors in AML compliance. The argument is centred on the internal auditor's proficiency, their exposure to key processes and their understanding of fraud indicators. Their position and abilities

enable them to assess an organisation's fraud and money laundering risks and to advise management of the necessary steps to take when indications of fraud and money laundering are present.

The design of internal controls that prevent, detect and mitigate fraud is the responsibility of management. However, arguments are made as to why internal auditors are an appropriate resource for assessing the effectiveness of AML controls which take their level of independence into consideration.

1.9.8. Conclusion and Recommendations

This chapter summarises the key issues of the research and examines whether or not the assumptions upon which the research is based are valid and can be substantiated. It provides holistic and integrated recommendations for reform that may be considered in the fight against money laundering. The research will also identify limitations and potential areas for further research.

CHAPTER 2

ANTI-MONEY LAUNDERING COMPLIANCE AND ANTI-MONEY LAUNDERING COMPLIANCE REVIEWS

2.1. Introduction

2.1.1. The Anti-Money Laundering Compliance Challenge

Following the financial meltdown of the late 2000s, the financial sector witnessed a tremendous shift in policy design and implementation. Unsound financial systems provide a safe haven for criminal activities (Shehu, 2010, p. 141). Although the AML focus had previously been on drug trafficking, banks later began to focus on terrorist financing. The importance arose of finding methods to fight terrorist financing, identifying the risks posed by customers with criminal intent, the need for changes to be made to products and services and recognising the locations where terrorist financing occurs. Logically, this created a greater sensitivity to money laundering risks in general (Pasley, 2011: 40).

After the dreadful events of 9/11, the AML world began a very steep learning curve. A significant AML evolution occurred that required improved coordination between governments and the private financial sector, more effective intelligence collection methods and the establishment of additional AML and CFT requirements for banks, mainly due to the USA Patriot Act (Pasley, 2011: 40).

The events of 9/11 accelerated the formation of a worldwide finance regime with overwhelming obligations resulting from various pieces of AML/CFT legislation. Financial institutions have been charged with a number of disclosure duties and faced with the end of bank secrecy privileges and the freezing of certain client accounts. These changes have placed banks under pressure and even threatened their survival (Leong, 2007: 150).

All organisations, regardless of their size, are vulnerable to companies and individuals intending to launder money but financial institutions are exposed to the

greatest risk (Sinason et al., 2003: 17). Financial institutions are now required to create AML procedures that go beyond their usual concerns and affiliates. This applies particularly to complex international organisations (Husisian, 2010: 17).

Concealing the proceeds of crime, which in many instances constitutes large amounts of money, requires fraudulent methods that have become extremely complicated and sophisticated over time. Such methods are continuously evolving and make use of the most recent technology (Angel & Demitis, 2005: 271).

Financial institutions play a critical role as intermediaries in the financial system. AML counter-measures rely on the cooperation of the financial sector. This level of reliance has increased continuously over the years to an extent that the information collected and analysed by financial intuitions, as part of their compliance requirements, is essential in any complex investigation (Ganguli, 2010: 1).

Simonova (2011: 347) point out that financial institutions play an invaluable role in preventing and detecting money laundering. Financial institutions can make it difficult and expensive for criminals to launder money. Thus financial institutions contribute immensely to the investigation of money laundering and the prosecution of those involved.

The culture of AML compliance also plays a crucial role. A focused, integrated and top-down approach for AML risk management and adequate controls effectively promote an environment where staff and managers are knowledgeable and aware of the risks. In order to promote accountability for risk management and control processes, AML responsibilities should be included in employee evaluation and compensation systems (Cromhout, 2002: 5).

Subsequently, banks have had to modify and update their existing AML programmes. However, banks still face extensive regulation and scrutiny. Serious penalties and fines may be imposed if they fail to comply with requirements (Maranto, 2006: 56). Moss and Seabron (2010: 44) state that credit unions have

worked hard to improve compliance programmes but compliance still remains a challenge.

As a result, compliance officers have a very difficult challenge. On the one hand, they are expected to provide clients with affordable, realistic and supportive services, while on the other hand, they must ensure compliance with law (De Koker, 2006: 38). Notwithstanding the challenges in place, there also appears to be a strong bonus driven culture by financial institutions which may impact how diligently financial institutions perform their checks for money laundering and fraud (Simonova, 2011: 351).

Some of the significant challenges facing financial institutions' management and audit committees include an enhanced risk management function, a greater emphasis on complex computer and information systems and the need to allocate resources to meet the compliance requirements (Raghavan, 2006: 35).

2.2. Money Laundering and Anti-Money Laundering Compliance Defined

The term "money laundering" originated in the 1930s when US Treasury agents were trying to apprehend Al Capone for fraudulent activities. At that time, very few people had running water and commercial laundries were common. Capone and his associates owned a chain of laundries in and around Chicago and disguised the earnings from their illegal liquor business as money earned from operating the laundries, hence the term "money laundering" arose (Mathers, 2004: 21).

According to Hopton (2006: 3), although many definitions of money laundering exist, they do not fully define the term. Money laundering is often seen in terms of what it is thought to be, rather than what it is. As a result, money laundering is not adequately defined. It may therefore be difficult for those with the responsibility to recognise money laundering to identify it in all its disguises.

The IMF (2001: 7-8) defines money laundering as "transferring illegally obtained money or investment through an outside party to conceal the true source". In the

South African context, the Independent Regulatory Board for Auditors (IRBA) (2011: 5) refers to money laundering as "any act that disguises the criminal nature or the location of the proceeds of a crime". However, South African legislation has broadened the concept to include "every act or transaction that involves the proceeds of a crime, including the spending of any funds that were acquired illegally".

In the context of South African criminal law, the term "money laundering" refers to a number of offences that are committed in terms of the Prevention of Organised Crime Act No. 121 of 1998 (POCA). The term overlaps with certain common law crimes (i.e. fraud, forgery and uttering) and statutory offences (i.e. corruption) (De Koker, 2002a: 27).

Section 1 of the Financial Intelligence Centre Act (FICA) defines money laundering as

> an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of this Act or section 4, 5 or 6 of the Prevention Act (FIC, 2001: 5).

To understand compliance, a clear vision of what it is and the part it plays in the financial services industry is necessary. In financial services, compliance is defined as the function of identifying relevant legislative, regulatory and best practice requirements and implementing the necessary systems and controls to ensure adherence to laws and regulations (Mills, 2008: 18).

According to certain Belgian regulators, compliance is defined as the implementation of a financial institution's integrity policy (Verhage, 2009: 116). An effective AML compliance programme is one that establishes internal controls that are developed in

response to an organisation's risk assessment and manages these risks according to the risk tolerance of the institution (Risk Solutions Financial Services, 2007: 4).

The FATF (2003b: 6), through the 40 Recommendations, endorses regular AML compliance of financial institutions by performing customer due diligence (CDD) checks, keeping records and reporting suspicious transactions.

Failure to fulfil the requirements leads to compliance risk which is defined as

> the risk of legal or regulatory sanction, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (Mills, 2008: 16).

2.3. Anti-money Laundering Preventative Measures

When financial institutions are not transparent, regulations and monitoring requirements are not followed. This makes criminal activity opportunities available and money laundering and terrorist financing (ML/TF) may thrive (IRBA, 2011: 20-21). Given the impact of the problem, understanding AML measures is vital. In government projects, AML is concerned with three levels in a hierarchy. These are the transnational, national and local organisations (Angel & Demitis, 2005: 271).

Transnational organisations are norm-producing and include the UN, the FATF and the Basel Committee on Banking Supervision. Transnational organisations serve as regulatory, administrative and supervisory bodies. Typical organisations at the national level are the central banks and financial intelligence units (FIUs). These organisations must comply with the norms established by the transnational bodies. Compliance also requires collecting information from the national level and communicating it to transnational bodies. Organisations at the local level normally include domestic banks and financial services such as exchange bureaus. The local organisations must comply with national requirements. They report to and are

monitored by organisations at the national level (Angel & Demitis, 2005: 271-272). The FAFT, on the other hand, is involved in the monitoring processes of members. This is mainly done in a two-stage process that includes self-assessment and mutual evaluations (Moshi, 2007: 4).

The IRBA is an example of a supervisory body responsible, in terms of the FICA, for supervising the compliance of accountable institutions, including registered auditors. The IRBA has general regulatory powers and duties under the Auditing Profession Act No. 26 of 2005. This Act imposes a responsibility to supervise compliance on all registered auditors along with their general statutory obligations. As a consequence, the IRBA is also charged with supervising registered auditors who are not accountable institutions but who have compliance obligations (IRBA, 2011: 20-21).

The bodies that regulate financial institutions include the Basel Committee on Bank Supervision (for banks), the International Organisation of Security Commissions (for security institutions and markets) as well as the International Association of Insurance Supervisors, the International Federation of Accountants and the Wolfsberg Group (Moshi, 2007: 5).

The Wolfsberg Group is an association of eleven international banks which came together in 2000 to draft AML guidelines. The aim was to develop standards for the financial services and related industries. The standards include the Know Your Customer (KYC) principle and AML/CFT policies. Various guidelines and AML principles have been drafted and shared among Wolfsberg Group members to manage money laundering risk and prevent money laundering in their institutions (The Wolfsberg Group, 2011).

International efforts to counter money laundering are motivated by an awareness of the consequences of the problem. The strategies developed to manage and mitigate the threat are a mixture of deterrence, detection and record keeping that collectively facilitates investigations (Shehu, 2010: 141).

The nature and complexities of controls used in an organisation will depend on the risks identified. There are many possible control methods but a few common examples include the KYC principle, monitoring systems for the timely detection of irregular activities, the identification of activities that warrant reporting using suspicious activity reports (SARs), investigations and the segregation of duties in the case of dual controls (Risk Solutions Financial Services, 2007: 7).

Goredema (2006: 14) gives the general framework of AML laws and institutional alignments. This is summarised in table 2.1 below. Each column refers to an AML pillar.

Table 2.1 General framework of AML laws adapted from Goredema (2006: 14)

Money laundering preventative measures	AML enforcement measures	Measures to foster trans-national cooperation
Customer due diligence	Criminalisation of predicate (underlying criminal) acts of money laundering	Awareness of global trends
Reporting obligations	Investigation of predicate activities and money laundering	Cooperation agreements/memoranda of understanding (MoUs) and real-time trans-national economic crime situation reviews
Regulation and supervision	Prosecution and punishment	Effective mutual assistance processes
Sanctions for non-compliance	Tracing and confiscating criminal proceeds	Trans-national structures to trace and confiscate proceeds of crime

Consistent with the view above, listed below are the common preventative measures used by a number of regimes. However, as expressed in section 1.8 on limitations

the research discusses only in greater detail customer due diligence, record keeping and transaction monitoring and reporting of suspicious transactions.

2.4. Customer Due Diligence

Financial institutions are required to pay strict attention to basic principles of good business practice. One principle is commonly known as “Know you customer” (KYC). Having a sound knowledge of a customer’s business, patterns of financial transitions and commitments will enable bank staff to recognise money laundering attempts (Nevin, 2000, p. 20). Primarily, customers are at the centre of the fight against money laundering and certain customers pose a higher level of risk than others (Risk Solutions Financial Services, 2007: 4).

Specific steps are necessary to adequately assess a customer. These include establishing the true identify of a customer, determining the source of their wealth and creating an accurate picture of what their relationship with the organisation should be. By knowing what is expected, financial institutions are in a better position to identify what is irregular activity and to determine whether it warrants a suspicious activity report (SAR). Institutions should refrain from treating customers differently but should evaluate all customer-related factors in determining an overall risk level for all clients (Risk Solutions Financial Services, 2007: 4).

The CDD measures involve verifying the customer’s identity using reliable, independent source documents or information and using reasonable measures to identify the beneficiary of a transaction (FATF, 2012: 14-15).

With reference to legal entities and arrangements, this should include understanding the ownership and control structure of the customer, obtaining appropriate information on the purpose and intended nature of the business relationship, conducting ongoing due diligence checks during the business relationship and scrutinising transactions to ensure that they are consistent with the institution’s knowledge of the customer, their business and risk profile, and, where necessary, the source of funds (FATF, 2012: 14-15).

Financial institutions are forbidden from keeping anonymous accounts or accounts in fictitious names. Furthermore, financial institutions are required to perform customer due diligence measures when establishing business relations; when carrying out occasional transactions; when there is a suspicion of money laundering or terrorist financing; and when the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data (FATF, 2012: 15).

CDD is one of the best defences a financial institution can use to guard against money laundering and other financial crimes. Often referred to as "knowing your customer," customer due diligence may include aspects of an AML programme, such as customer identification and enhanced due diligence (EDD) as necessary. CDD is fundamental to SAR requirements because data collected during the CDD process is transferred by means of the report (Geister, 2010: 3).

Maranto (2006: 56) argues that it is no longer merely about knowing one's customers but also about knowing one's employees. Maranto (2006: 56) points out that most money laundering cases involve employees of a bank thus banks need to be aware of certain aspects of their employees' lives while having controls in place to ensure proper employee conduct.

2.5. Record Keeping

It is a legal requirement that financial institutions maintain records on transactions and information obtained through the CDD measures. These records should be readily available to domestic authorities. Financial institutions are required to maintain all necessary records on transactions, both domestic and international, for a minimum of five years. The records must be sufficient to reconstruct individual transactions, provide evidence for prosecuting criminal activity and include the amounts and types of currency involved (FATF, 2012: 15).

Financial institutions are also required to keep all records obtained through CDD measures, for example, copies or records of official identification documents (passport, identity card, driver's license or similar documents), account files and business correspondence including the results of any analysis or inquiry performed

to establish the background and purpose of complex, unusual or large transactions. The records must be kept for at least five years after the business relationship has ended or after the date of the transaction (FATF, 2012: 15).

2.6. Monitoring and Reporting of Suspicious Transactions

According to Van de Westhuizen (2008: 30-1), on 14 March 2008 the Financial Intelligence Centre (FIC) issued a guidance notice on suspicious transaction reporting in terms of section 29 of the FICA. Section 29 of the FICA imposes a reporting obligation on any person who carries on business, manages and is in charge of a business, is employed by a business and who knows or ought reasonably to know or suspect certain information regarding money laundering.

Most jurisdictions with money laundering regulations in place require financial institutions, designated non-financial institutions and related professions to have an AML compliance officer. Furthermore, employees are required to report any suspicious activities to the money laundering officer who will then escalate the matter to the relevant FIU's (Mugarura, 2011: 184).

Angel and Demitis (2005: 278-279) argue that suspicious transaction reporting is the first line of defence in an organisation's local system. The penalties for non-compliance are important as they ensure effectiveness. If a financial institution suspects or has reasonable grounds to suspect that certain funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required by law to report this promptly to the FIU (FATF, 2012: 19).

To ensure that employees understand and report suspicious transactions, they should receive appropriate training on AML procedures, reporting lines and as to what constitutes a suspicious transaction. The recommendations also require that financial institutions pay special attention to all complex, unusual and large transactions and any unusual patterns in transactions (Mugarura, 2011: 184).

However, the major problem which many countries face with their reporting procedures is that the term "suspicious transaction" is vague and subjective and can

be interpreted differently by various stakeholders. As a result, the decision is based on KYC (Know your Customer) principles after profiling a customer's transactions and on knowing their financial status and activities in order to identify any irregularities (Angel & Demitis, 2005: 279).

Van der Westhuizen (2008: 30-31) highlights the fact that despite the challenges, certain transactions are possible red flags for unusual and suspicious transactions, and as such should be reported by financial institutions. Such transactions include deposit of funds with request for immediate transfer elsewhere; payment of commissions or fees that appear excessive in relation to those normally payable; unwarranted involvement in structures such as trusts and corporate vehicle transactions; the buying or selling of securities with apparent concern for making a profit or loss avoidance; customers having unusual knowledge of the law in relation to suspicious transaction reporting; customers changing a transaction after learning that they must provide a form of identification; and the involvement of significant amounts of cash in circumstances that are difficult to explain.

Maranto (2006: 56) emphasises the need for banks to use technology to run their business and to support compliance measures, particularly in transaction monitoring. Banks are required to continuously ensure their system provides valuable management output, evaluates and highlights transactions based on the level of risk and uses relevant criteria to identify suspicious activities. Costanzo (2008: 56), on the other hand, expresses a different viewpoint, stating that the identification of suspicious transactions is a labour-intensive exercise and should primarily be outsourced.

Identifying unusual and suspicious transactions is an ongoing process that requires continuous monitoring requiring the latest software and adequate staff training. However, combating money laundering can sometimes be a reactive exercise. Despite the efforts undertaken by various financial institutions, money laundering is constantly evolving in nature as a result those responsible for identifying it often have insufficient knowledge to adequately identify money laundering in all its disguises (Hopton, 2006: 3).

2.7. A Risk-Based Approach to Anti-Money Laundering Compliance

2.7.1. The Purpose of a Risk-Based Approach

It is well understood that money launderers will go to great lengths to make their transactions indistinguishable from legitimate transactions. It thus becomes very difficult and sometimes impossible for financial institutions to distinguish between legitimate and illegitimate transactions (Wolfsberg Group, 2006: 1).

By properly applying a risk-based approach, countries must ensure that measures to prevent or mitigate money laundering and terrorist financing are sufficient for the risks identified. This approach helps in efficient allocation of resources in AML/CFT and in the implementation of risk-based measures. Countries should also require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective management action to mitigate money laundering and terrorist financing risks (FATF, 2012: 11).

According to the FATF (2012: 11), countries should identify, assess and understand the money laundering and terrorist financing risks and management should take necessary action to coordinate risk assessments and apply resources to ensure that money laundering and terrorist financing risks are mitigated effectively within financial institutions.

Although many financial institutions fear the consequences of not following regulations and create a robust, rigid framework that seeks to address every possible scenario but fails to mitigate the risks in reality. Employees are driven by targets and performance measures but there is little emphasis on how well they have applied themselves to mitigating the risks of money laundering and terrorist financing (Killick & Parody, 2007: 211).

In acknowledging the challenges, the BSA/AML requirements are changing the emphasis of corporate governance and functions in financial institutions. Integration

possibilities in the internal control structures are evolving in response to regulations and the need to maintain a competitive advantage (Raghavan, 2006: 29).

The ongoing threat of money laundering in financial institutions can be most effectively managed by understanding and addressing the potential risks associated with customers and transactions (Wolfsberg Group, 2006: 1). As with most compliance issues, AML compliance requires sound knowledge of risk profiles. Such compliance should at least entail a careful review of a financial institution's business, product lines, type of customers, activities and operations to determine where problems are most likely to arise (Husisian, 2010: 16).

The concept of risk is an essential part of business theory. In 2003, the concept of risk was explicitly introduced into the AML FAFT standards and has become a central concept in various AML regimes (Simonova, 2011: 346). In December 2005, representatives of the FAFT and of the banking and securities sector agreed to establish a risk-based approach to combating money laundering and terrorist financing as part of its private sector programmes (FATF, 2007: 1).

It is worth noting that risk has always been a fundamental part of AML policies, even in a rule-based approach. However, the concepts of risk, risk assessment and risk management have been embraced and are now central themes in the preventative AML/CFT policies (Ross & Hannan, 2007: 107). The term 'risk-based' is found throughout the FATF 40 + 9 Recommendations but few examples explaining what the term means are given and this may have partly been due to the many poorly implemented systems and unclear definitions of risk based approach in the FAFT 40+ 9 recommendations (Killick & Parody, 2007: 211).

Ross and Hannan (2007: 107) assert a that risk-based approach in preventative AML/CFT policy is centred on the actual risk in present in the environment of financial and credit institutions and on ensuring that measures are adequate for the level of risk that may exist.

To quantify risks and allocate resources appropriately financial institutions should conduct risk assessments of its products, customer base, lines of business and geographical locations. Based on the results of such an assessment, smaller regional financial institutions may operate effectively with one centralised department while larger organisations with higher risk levels need a multifaceted approach and should maintain separate compliance functions for each line of business (Axelrod & Ross, 2012: 71).

By conducting a thorough risk analysis, senior management will be able to identify weaknesses in the system and determine the likelihood of money laundering and the severity of the consequences. A good programme will manage risks according to the tolerance level of the institution (Risk Solutions Financial Services, 2007: 4)

The diagram below (Figure 2.1) illustrates and summarises the risk assessment links and cycle in an AML risk management programme (FATF, 2007: 38).

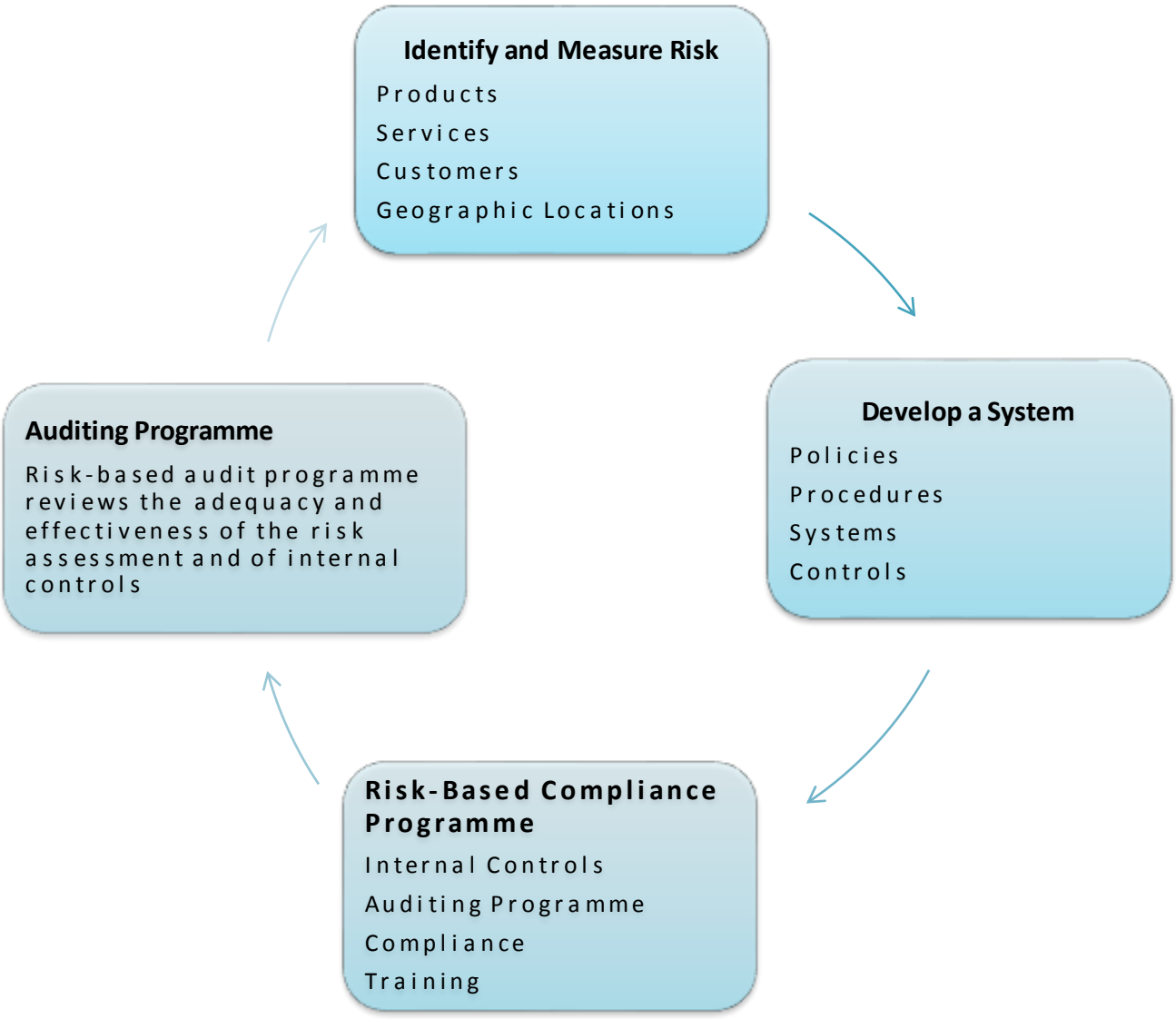

Figure 2.1 The risk assessment cycle of an AML management programme (FATF, 2007: 38)

Axelrod and Ross (2012: 71) point out that risk assessments are not static in nature. Financial institutions are advised to conduct a periodic review (annually, or more often, depending on the level of risk) and update their risk assessments to manage new and emerging risks and regulatory changes. Risk assessments should accommodate changes in a financial institution's products, customer base and markets.

According to Maranto (2006: 56), to maximise their effectiveness, AML programmes should be implemented for all activities, business lines and entities. They should also be based on a comprehensive view of risk including identification of risk sources, risk ranking and the management of specific programme functions.

Maranto (2006: 56) argues that a risk-based analysis involving all business lines and products can contribute significantly to identifying and implementing proper procedures and to address potential weaknesses. Establishing a comprehensive risk-based AML programme may be time consuming but if a bank has a well-documented risk-based methodology it should be able to justify its CDD decisions, transaction monitoring and AML compliance efforts.

Killick and Parody (2007: 211) show that a risk-based approach has two main requisites. The first requirement is that regulators understand the approach well and that senior managers are responsible for ensuring that their systems are appropriate and thorough. The second requirement is that no two systems are the same. The development of an effective AML compliance programme is not a 'one-size-fits-all' approach. It must fit the nature of the business activity and the type of risk the institution encounters (Axelrod & Ross, 2012: 71).

The FAFT (2007: 4) shares a similar viewpoint: no two financial institutions are the same and they are unlikely to adopt the same AML processes. Financial institutions must therefore be given an opportunity to make a reasonable evaluation of their own systems.

Killick and Parody (2007: 211) state that the terms "appropriate" and "proportionate" are the keys to a system that fits its purpose. An appropriate system must be relevant to the type of business and satisfy all legal requirements. A proportionate system includes intensive measures that mitigate the risk as far as possible and in relation to the risk profile.

Using a two dimensional matrix, such as the one shown in Figure 2.2 below, a product, customer or type of threat can be mapped to determine its risk profile in relation to an organisation (Killick & Parody, 2007: 211).

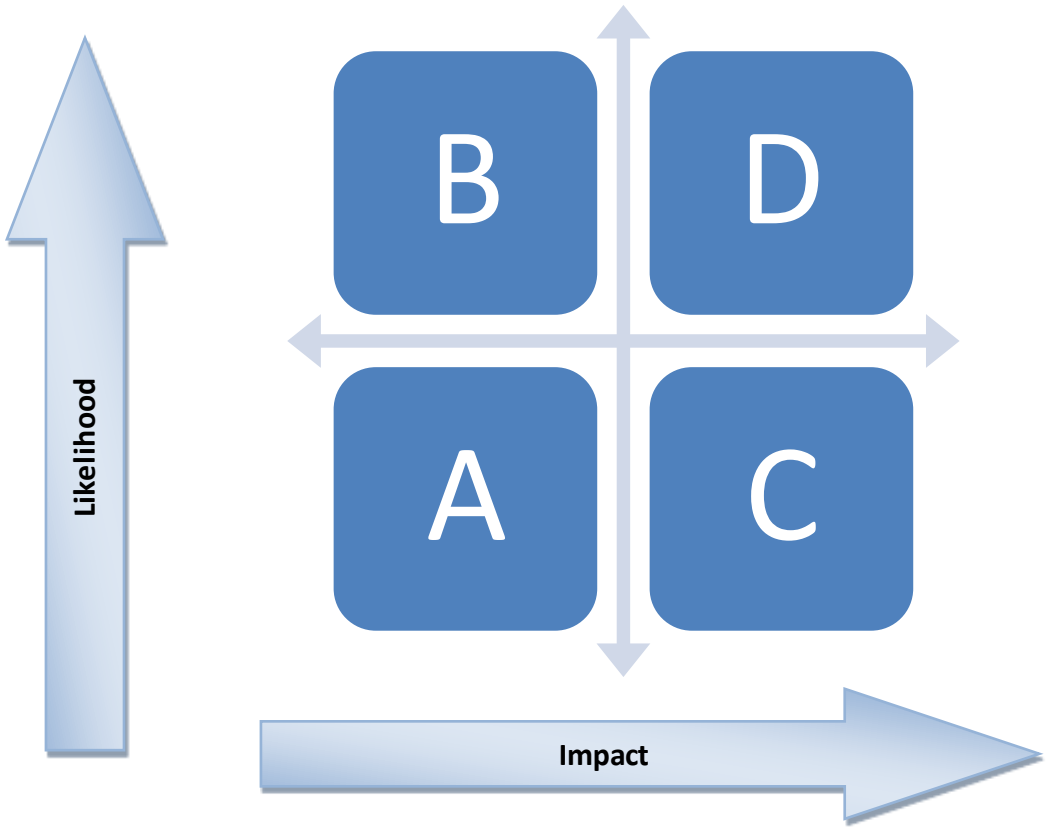

Figure 2.2 *A* risk-profiling matrix (Killick & Parody, 2007: 211)

The matrix has four quadrants. Each quadrant contains certain risks. Risks in the top right quadrant (D) are prioritised because of their greater likelihood and more serious impact. By contrast, the risks in quadrant D may never be fully mitigated. Consequently, in mitigating such risks financial institutions would have to implement severe controls and restrictions that would prevent them from managing their business successfully, as the only means of mitigating all these risks would prevent any business from being conducted. The lower left quadrant (A) represents risks that have a low impact and are less likely to occur. Accordingly, the risks in quadrant B and C are the ones to which a firm should dedicate effort and resources (Killick & Parody, 2007: 211).

According to this approach, resources and attention should be directed to the most likely and most serious risks. These risks will be subject to enhanced procedures (FATF, 2007: 2). Similarly with the risk based approach to money laundering, risk based auditing requires that auditors should test the entire programme but particular focus should be placed on high risk areas. Previous auditing reports must be referred to so that the auditor can confirm that corrective actions recommended in the past have been implemented and risks are effectively managed (Risk Solutions Financial Services, 2007: 9).

2.7.2. Benefits and Challenges of a Risk-Based Approach

The acceptance and implementation of a risk-based approach to combat money laundering and terrorist financing can be beneficial for all parties involved (FATF, 2007: 3). Firstly, in comparison with a rule-based approach, a risk-based approach is far more flexible (Muller, Kalin, & Goldsworth, 2007: 97). A risk-based approach requires discretion on the part of an entity in identifying the level of risks, as a result, quality reports would be produced from a risk-based approach as opposed to defensive reporting (Ross & Hannan, 2007: 107).

Through cooperation and understanding between authorities and financial institutions, money laundering can be more effectively managed especially by means of risk-based processes. Entities generally know where the highest risks are and can dedicate resources and efforts to those specific risks instead of spending resources on areas of low risk (FATF, 2007: 3). Another advantage of a risk-based approach is how its design makes it more difficult for criminals to use a financial institution because of the increased attention given to the high-risk activities criminals attempt to exploit (FATF, 2007: 3).

Although risk-based approaches have many advantages they also have challenges. A risk-based approach is not a straightforward option as there are hurdles to be overcome in implementation. Some challenges are inherent to risk-based systems (FATF, 2007: 3). A risk-based approach has flexibility but is also demanding

because institutions are expected to develop their own internal risk policies (Van den Broek, 2011: 173).

A risk assessment is the foundation for developing all measures and mitigating controls in a risk-based approach. However, if the risk assessment is not performed properly and the recommendations are unsound, the entire risk-based approach will inevitably be flawed (Geary, 2009: 215-216). Another primary concern is that there is no common risk language or vocabulary and no explicit understanding of what risk is among the different stakeholders. For instance, institutions in the same country and individuals in the same institution may each refer to risk and its related concepts in a different sense even though they use the same terms (Simonova, 2011: 349).

Quantifying risk and the probability of a fraudulent event occurring is a major challenge. Historic data may be useful for developing certain types of models but the same cannot be said of AML/CFT. Nevertheless, banks and other financial institutions are expected to take all reasonable measures to manage AML/CFT risks in their businesses (Johnson & Carrington, 2006: 54).

When regulators monitor AML/CFT compliance in a rigid manner, without considering the appropriate and proportionate methods put forward by a risk-based approach, the industry will soon adopt a model that is more compliance-based, regardless of its merits (Killick & Parody, 2007: 215).

Another issue raised is that staff who conducts assessments may not be experienced or authorised to perform them. Some staff members are uncomfortable with making risk-based judgments and this may lead to overly cautious decisions or an unnecessary amount of time spent on documenting the rationale behind decisions (FATF, 2007: 4-5).

Geary (2009: 215-216) states that the AML/CFT rules are silent on the need to consider the risk posed by employees and this is a significant gap. Other aspects of the AML/CFT show that employee risk needs to be assessed in order to implement a risk-based approach.

2.8. Performing an Anti-Money Laundering Compliance Review

AML audits are intended to test a financial institution's adherence to a compliance programme and the fulfilment of its regulatory responsibilities. The topics covered in AML reviews differ depending on the specific AML programme and institution. Commonly, AML compliance reviews seek to ascertain that

- the company maintains all accounts in accurate and legitimate names
- an organisation records and verifies the identity of its customers using reliable documents and supporting information in line with the relevant regulations
- the AML compliance programme policies and procedures in place effectively handle the financial institution's AML responsibilities
- the current programme's risk assessment is up-to-date and applicable to the existing products, services, customers and geographical locations involved
- the financial institution adheres to all reporting requirements
- staff training is appropriate and complete
- the financial institution maintains records for the minimum required period (five years) after the termination of an account or a relationship
- financial institutions use appropriate information systems to identify issues relating to large transactions and to aggregate daily currency transactions et cetera
- procedures are in place to detect efforts to evade controls
- the financial institution has properly prepared all reports necessary for AML compliance
- compliance procedures are followed correctly, especially for high-risk activities
- the information used to evaluate suspicious activities and to generate SARs is promptly identified, referred to compliance personnel and thoroughly investigated (Husisian, 2010: 20-23).

Shonk (2007a: 7) argues that federal banking regulators must vigorously scrutinise an institution's AML programme regardless of the institution's size. Small and large banks must continually fine tune their AML efforts. Special attention must be given to

recent enforcement actions and the AML auditing functions to help banks minimise risk and improve compliance.

2.9. Challenges and Limitations Identified in Current Anti-money Laundering Compliance Reviews

The FATF states:

> [I]f a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU) (2003b: 5).

The FATF recommendations place a reporting duty on non-financial businesses and professions. According to the FATF (2003b: 6).

> Lawyers, notaries, other independent legal professionals and accountants are required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d) however when *acting as independent legal professionals* (lawyers, notaries, other independent legal professionals and accountants), are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege

Lawyers, notaries, accountants and other independent professionals have access to client's secret information. However, AML compliance requirements appear to be in conflict with the privilege of confidentiality in communication between these professionals and their clients (Ping, 2006: 66).

Lawyers, notaries, other independent legal professionals and accountants are sometimes unwilling to gather precise information on their clients such as the origin of a client's money to protect themselves. This has a detrimental effect on their professional activities (Ping, 2006: 66). Thus, instances of possible deviations or anomalies may not be identified or reported.

Another issue is that there are inherently a number of limitations when comes to identifying money laundering. Though the traditional model is useful however it does not adequately cover all situations in which money laundering occurs due to insufficient skills and knowledge by staff (Hopton, 2006: 3)

It is also prudent to ask whether the board and management have instilled a culture of compliance that ensures adherence to bank policies and procedures in their institution. Another important question asks whether employees have received the appropriate level of AML/CFT training (Garces, 2010: 58). Relevant criteria to be considered include employees' knowledge of legislation and regulations and the institution's record in terms of compliance, bribery, front-running and insider trading (Simonova, 2011: 351).

Shonk (2007: 8) maintains that although AML compliance reviews are performed there are potential areas of concern. These include limited transaction testing; insufficient scope; a general compliance focus rather than a risk management focus; a lack of organisation-wide assessment; a generally weak assessment of account monitoring and the SAR process; as well as limited evaluation of training and limited structured review.

Although a risk-based approach is implemented in certain instances, AML/CFT rules are silent on the need to consider the risk posed by employees, which is a significant gap. Other aspects point toward the conclusion that employee risk needs to be assessed in order to implement risk-based approach to managing the problem (Geary, 2009: 215-216).

Compliance officers often face the hurdle of convincing directors, senior managers and other stakeholders of the scope of AML/CFT and the need for compliance, particularly in terms of budget. At times, the AML compliance officers may not know what is expected and succumb to the temptation of using an AML policy issued by a trade association without taking into consideration the day-to-day operations of the business (Beaumier & Shah, 2003: 15).

Another common problem is that financial institutions apply AML regulatory requirements in a fragmented manner. For example, KYC/CDD and EDD standards are developed without considering the need for risk assessment or the purpose of monitoring. In these circumstances institutions often need to revise the AML programme to ensure full compliance (Beaumier & Shah, 2003: 15).

Ganguli (2010: 2) shares a similar viewpoint to Beaumier and Shah and highlights that a framework of rules is often fragmented. Systems tend to borrow certain elements from each other and may rely on these to a certain extent but they do not constitute a fully integrated system of rules and regulations.

2.10. Summary

Although efforts have been made to improve AML programmes, compliance still remains a challenge for most, if not all, financial institutions (Moss & Seabron, 2010: 44). Due to unsound financial systems and the financial meltdown, in the late 2000 the financial sector witnessed a tremendous shift in policy design and implementation (Shehu, 2010: 141). Financial institutions were subsequently scrutinised as intermediaries in the financial systems (Ganguli, 2010: 1).

This chapter highlighted a number of strategies to counter money laundering. The strategies entail a combination of deterrence, detection and record keeping to assist further investigations (Shehu, 2010: 141).

As banks began to focus on terrorist financing, new risks involving their customers, products and locations surfaced. This created a greater sensitivity to money laundering risks in general (Pasley, 2011: 40). Risk-based approaches to money

laundering and their importance were examined. Maranto (2006: 56) highlights that AML programmes should be implemented for all activities, business lines and entities. They must also be based on a comprehensive view of risk that includes identifying the sources of risk, classifying risks and managing specific programme functions.

The chapter also addresses and explains the objectives of AML compliance reviews and how they are performed. In conclusion, the chapter highlights limitations and challenges commonly identified in AML compliance reviews.

The research provides a number of limitations that are currently characteristic of the fight against money laundering notably the role of lawyers, notaries, other independent legal professionals and accountants who may present a hurdle to effectively managing and controlling money laundering (FATF, 2003b: 6).

CHAPTER 3

THE NEED FOR INDEPENDENT ANTI-MONEY LAUNDERING COMPLIANCE REVIEWS

3.1. Introduction

3.1.1. Non-Compliance by Financial Institutions

The fight against money laundering has grown exponentially, effectively becoming an industry in its own right. In recent years the fight has spread from banks to other financial activities and other areas including company and trust fund management (Killick & Parody, 2007: 211). In response, policies are geared towards increasing compliance by establishing comprehensive AML/CFT regimes (Gardner, 2007: 329). Non-compliance means ineffectiveness and the term “compliance” has become synonymous with AML/CFT (Gardner, 2007: 329).

In keeping with international standards, financial institutions build compliance functions and assign compliance officers to advise management on compliance issues and assist them to ensure that the institution and its employees comply with applicable laws (De Koker, 2006: 38). Nevertheless, compliance still remains a challenge for most, if not all, financial institutions (Moss & Seabron, 2010: 44).

In October 2005, Banco de Chile (The Bank of Chile) was fined US$3 million for violating the American Bank Secrecy Act (BSA). The bank’s customer identification programme was deficient and did not require a customer identification number. Further to this the bank did not provide customers with information on regulation requirements, conduct independent testing, prescribe when a suspicious activity report (SAR) was to be filed or define parameters for account closure in the absence of customer identity verification (Bryne & Kelsey, 2006: 9).

Also in October 2005 a US$2,5 million fine was issued to Oppenheimer & Company Inc. for deficiencies in its BSA programme requirements, including failures to

properly identify clients and to report suspicious transactions. In February 2006, the Officer of the Comptroller of Currency (OCC) announced that consent orders had been made with Pinebank Asset Management (New York), National Association (Miami) and Summit National Bank (Atlanta) for AML deficiencies (Bryne & Kelsey, 2006: 11).

In another case involving Riggs Bank in America. This was perhaps a special case as it does not only relate to failures in the institution's internal system of controls but was characterised by intentional actions by bank senior staff to facilitate efforts to disguise the true source of funds by General Pinochet, the ex-Chilean dictator (Johnson & Carrington, 2006: 53). Likewise, in 2012, HSBC underwent investigations into allegations that Mexican drug cartels and terrorist groups used the bank to launder money. Consequently, HSBC announced that it would set aside US$700 million to cover any fines, settlement or legal fees it might incur from the US Senate investigation (Mont, 2012: 18).

International banks have been a target for severe criticism for failing to check the true identify of wealthy customers, as well as the source of their income. Banks have been accused of not assessing and reporting suspicious financial transactions (Mohamed, 2002: 68).

Johnson and Lim (2002: 8) emphasise that banks are vulnerable to money laundering as they provide three main advantages to criminals: convenience, accessibly and security. Criminals can have access to international and electronic payment systems that do not require them to carry large amounts of cash.

3.1.2. The Costs and Implications of Anti-Money Laundering Compliance

Banks and other participants have become used to ever-increasing regulations but object to the burden they face in fulfilling the many regulatory requirements. Banks and other financial services are concerned about the implementation costs associated with money laundering, which place a large burden on the industry, particularly on smaller financial institutions (Geiger & Wuensch, 2007: 92).

The current hurdle is that risk management frameworks increase costs for the private sector. Institutions subject to regulations must then develop procedures and systems, keep them up-to-date and train their staff to apply the procedures and systems. Resources and expertise are required to gather and interpret information on risk, develop procedures and systems and to train employees at both the institutional and national level. The disadvantages of this approach are that it may cause a level of uncertainty regarding expectations, difficulty in applying a uniform regulatory treatment and possibly lead to a lack of understanding by customers regarding information required when opening an account (FATF, 2007: 4-5).

Compliance costs are significant and increasing but they are manageable for larger banks. Smaller institutions struggle to absorb the increasing costs. These costs inevitably weigh on overall bank profitability and may harm credit availability (Mont, 2012: 18). The burden on smaller banks is estimated to be more than twice that of bigger banks. Small banks are heavily penalised in comparison with larger institutions. As a result, regulators considered how costs and benefits may be balanced for smaller institutions (Geiger & Wuensch, 2007: 92).

The costs of complying with AML regulations have increased exponentially over the years and have had a severe impact on smaller businesses. Smaller businesses have had to comply with all sorts of “improved” regulations which increase compliance costs fivefold (Angel & Demitis, 2005: 271).

Maranto (2006: 56) highlights the fact that AML-related penalties have been increasingly significant in recent years and agreements between banks and regulators have become more complex and detailed. Shonk (2007a: 7) indicates that failing to comply with AML requirements may result in regulatory actions, monetary fines and denial of business expansion requests. Such penalties may also harm an institution’s reputation with investors, customers and communities.

Reputation is always at risk and this means an institution may be damaged by one or more than one event including negative publicity about its business practices,

conduct or financial condition. Such negative publicity, whether it is true or not, may impair public confidence in the company, result in expensive litigation and leading to a decline in its customer base, business and revenue. The impact on reputational may lead to damaged trust, draw further scrutiny from regulators, raise questions on the ethics, values, practices and internal standards of the organisation (Binneman, 2012: 33).

The failure to test and correct AML programmes accordingly may lead to an intense burden that goes beyond monetary penalties. Violations may result in strict regulatory supervision of the financial institution's compliance efforts and programme. Depending on the seriousness of non-compliance, outside consultants may be required. It is likely that strict and regular reporting to the institution's board of directors would be required of the AML compliance programme. In turn, the board would be required to respond to all reports, make recommendations and follow up on findings (Risk Solutions Financial Services, 2007: 9).

The compliance management systems that large financial institutions employ are highly complex and expensive in the same manner the systems must also have a flexible design (De Koker, 2006: 38). Increased compliance scrutiny regarding additional laws and regulations is a further burden because banks and other financial institutions have had to increase their compliance staff to develop a more sophisticated technology and devote other resources to advice and monitor on AML/CFT compliance related matters (Pasley, 2011: 42).

Similar concerns are shared by regulators in terms of the cost burden on banks and other financial institutions in relation to AML/CFT compliance. There is a direct cause and effect relationship between the expense incurred and the prospect of reduced income. This has resulted in a decline in certain lines of business and, more importantly, intangible inconvenience costs for customers (Johnson & Carrington, 2006: 57).

Inevitably banks have to examine the costs versus return benefits associated with AML/CFT compliance. The objective to maintain competitive value for shareholders

remains but there is also a concern regarding the costs associated with compliance. Institutions must ensure that compliance does not bring forth unnecessary barriers to conducting business with customers (Johnson & Carrington, 2006: 56).

De Koker (2006: 38) point out that compliance officers have an immense challenge to advise and implement compliance risk management systems that are affordable, realistic and supportive to business processes and objectives. However they also must ensure compliance with law.

Verhage (2008: 15) states that the compliance industry requires an entrepreneurial approach to money laundering. The supply side of the compliance market is built around a number of services that provide support to AML and compliance officers. These services are derived from software providers (to enable transaction monitoring), trade information bureaus (for information on potential clients), a database of high risk-individuals (for background thorough checks on potential individual clients), advisors (including advisory firms such as KPMG and E&Y) and the training and education of staff and compliance officers.

Software vendors have identified a commercial opportunity and now offer more cost-effective AML solutions to smaller banks and financial institutions. Service providers make technology available through an outsourcing arrangement. Outsourcing has however confronted institutions with the question of which activities can comfortably be handled by third party and which should be handled internally (Costanzo, 2008: 24-26). Both money laundering and AML have now become fully blown industries, each a ‘sustainable’ activity in their respective legal and illegal economies (Angel & Demitis, 2005: 271).

Though there are no definite figures on the financial burden incurred in the fight against money laundering imposed on financial institutions and ultimately on consumers. It remains unclear whether this cost has resulted in a truly effective system against money laundering (Killick & Parody, 2007: 210).
A number of banks have had to discontinue their relationships with organisations, predominantly those in the financial services, because banks believe that regulatory

risk and administrative costs are extremely high (Maranto, 2006: 56). Dollar and Shughart (2011: 20) argue that commercial banks face the most stringent requirements resulting from the AML mandates in the US Patriot Act of 2001 although considerable compliance costs are borne by the entire banking industry.

However, in scenarios where management fails to recognise or underestimate risk, a culture of non-compliance may slowly develop in a financial institution. Inadequate resources may be allocated to compliance testing and this leads to potentially significant compliance failures (FATF, 2007: 1).

3.2. Defining Independence in Anti-money Laundering review terms

The April 2009 *South African Government Gazette* (2009: 310) explains independence in terms of the Companies Act No. 71 of 2008. According to the *Gazette*, independence is defined as maintaining impartiality in the exercise of authority and in performing functions. Independence thus means that there is no conflict of interest.

The King III Report (2009: 52) defines independence as "the absence of undue influence and bias which can be affected by the intensity of the relationship between the director and the company". Another source defines independence as "having no relationship to the corporation that may interfere" in the performance of duties (Ligthtle & Bushong, 2000: 39).

Internal auditing principles indicate that independence requires operation at the highest hierarchical level to ensure objectivity in activities (Iovitu, Borisov, & Calanter, 2013: 299). Another definition describes independence as "freedom from material conflicts of interest that threaten objectivity", it is a state where threats to objectivity are managed to the extent that the risk of ineffective internal services are acceptable and controlled (Christopher, Sarens, & Leung, 2009: 201).
In the AML context, independent auditing refers to a review by persons who are not party to the AML/CFT policies and procedures. This is not only relevant to banks but to other financial institutions as well (Delston, 2007: 5).

The US Treasury (2006: 2) indicates that AML reviews should provide a fair and unbiased appraisal of the elements of an entity's programme. Independent auditing is one of the four pillars of an AML programme, along with a system of compliance, controls, a designated AML compliance officer and continuous AML training (Delston, 2007: 5).

An auditing function that performs AML compliance reviews must be managed independently, objectively and sufficiently resourced to provide an impartial assessment of the adequacy and compliance of the bank's established policies, processes and procedures (FATF, 2009b: 128).

Verhage (2009: 116) describes the compliance function as an internal independent function in an organisation which aims to investigate and advance the observance of regulations related to the integrity of banking.

Delson (2007: 6) is of the opinion that independence not only means being outside the specialist AML teams but that it also requires a function to have a separate reporting line. This implies that the compliance team not having the responsibility of drafting and implementing the financial institutions' AML programme.

Shonk (2007a: 8) shares a similar viewpoint to Delson: AML audits cannot be performed by individuals administering the AML programme or those supervised by the compliance officer. However, there are instances where small institutions with limited staff may have difficulty conducting an internal audit that is sufficiently independent from its compliance function.

To ensure independence, the compliance officer should have direct access to support from the chief executive officer (CEO) of the bank. The compliance officer must report non-compliance with laws and regulations or supervisory requirements to the CEO, board of directors and audit committee in a timely manner (Banks Act Regulation 49(4) (b) and (d)) (FATF, 2009b: 129).

3.3. Independent Anti-money Laundering Compliance Reviews – an Essential Element

Regulators generally require and favour AML programmes with meticulous compliance and transaction monitoring functions. However a thorough AML programme should not be confused with independent AML testing (Sartip, 2008: 58). Cromhout (2002: 5) stresses that to ensure good governance and proper risk management, particularly with regard to money laundering, a comprehensive, and customised AML compliance programme should be developed that includes an independent testing programme.

The FATF (2012: 78) states that financial institutions should conduct independent audits to test their own AML systems. Although the FATF Recommendations do not indicate who should perform independent reviews, they are highlighted as an AML priority.

It is thus critical to review the internal controls, policies and procedures designed to mitigate AML/CFT risks and to determine the extent to which such policies and procedures have been implemented. While most banks conduct their own AML/CFT risk assessments it is important that an independent review be performed as well (Garces, 2010: 58).

The value of an effective independent compliance programme review cannot be overemphasised. Independent reviews assist the board of directors and senior management by identifying areas of weakness which require additional controls (FDIC, 2008).

Khan (2007: 46) maintains that independent testing by knowledgeable internal auditors is critical to ensuring that AML/CFT programmes are robust and fully aligned with regulatory requirements. The testing of these core programmes should be interconnected and integrated with a well-defined strategy that has a risk-based perspective and involves the whole business.

In June 2008, amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act came into effect. These included the requirement for reporting entities to conduct an independent review of their compliance policies, procedures, risk assessment and training programme at least every two years (PwC, 2010: 1).

Independent annual audits or other independent tests are thus additional safeguards required for pre-empting negative regulatory examination findings. The degree of integration between the business, its compliance function and the internal audit is often the key to effective AML programmes that mitigating risks (Axelrod & Ross, 2012: 73).

PricewaterhouseCoopers (PwC) (2010: 1) points out certain pitfalls that should be avoided when an AML review is performed. These are that the review not be conducted by a person who is not sufficiently knowledgeable and trained in terms of AML/AFT controls and requirements and that the review is conducted by an individual who is truly independent of the compliance functions and who has no conflicting roles.

A number of auditing and review deficiencies were noted when examining AML audit processes. Generally, AML reviews lacked independence and were performed by unqualified auditors (Shonk, 2007: 8). Other pitfalls to be avoided include an insufficient review scope that does not cover all products or business, insufficient sampling and testing of transactions and clients, the failure to formally report the results of the review to senior management when review processes and findings are inadequately documented (PwC, 2010: 1).

It is evident that financial institutions are integral to the fight against money laundering. More so It is equally crucial that organisations implement effective independent review programmes to assess the quality of their AML/CFT programmes (Khan, 2007: 48).

Based on the views raised, it is evident that independence and competence are two pivotal components of AML reviews. One could conclude that it is not merely about ticking the right boxes but rather it is about having adequate, competent and independent staff to perform AML reviews.

3.4. Conducting an Independent Anti-Money Laundering Compliance Review

3.4.1. What Should Be Done During the Review?

Auditing is important to ensuring that the compliance function is effective. In instances where compliance processes are generally demonstrated to be efficient, the regulator may be persuaded to reduce fines incurred when non-compliance does occur (Terblanché et al., 2008).

The primary purpose of the AML independent review should be to provide a fair and unbiased assessment of each of the required elements in the organisation's AML programme including the policies, procedures, internal controls, record keeping, reporting functions and training. The review should comprise of internal control transactional systems testing, procedures to identify control breakdowns and weaknesses, and to recommend to management appropriate corrective actions that will mitigate the risks identified. For instance, if the programme requires that an employee or category of employees should be trained on a particular aspect of money laundering once every six months, the independent testing should determine whether the training occurred and whether the training was adequate while taking into consideration the level of risk involved (Department of the Treasury, 2006: 2-3).

As part of the responsibility of the designated compliance officer, the review also should cover all of the AML programme actions taken. These actions include, for instance, determining the level of money laundering risks faced by an organisation, the frequency of BSA anti-money laundering training for employees and the adoption of procedures for implementation and oversight of programme-related controls and transactional systems (Department of the Treasury, 2006: 2-3).

Independent testing should, at minimum, include a review of the bank risk assessment according to its risk profile, appropriate risk-based transaction testing to verify the bank's adherence to record keeping and reporting requirements and an evaluation of management's efforts to resolve violations and deficiencies noted in previous audits (Anonymous, 2008: 3) The scope of these AML reviews, whether conducted by compliance or internal auditing staff, should be comprehensive enough to uncover potential areas of vulnerability and this requires target testing high-risk areas and ongoing monitoring (Axelrod & Ross, 2012: 73).

It is equally necessary for the audit team to understand the organisation's products and delivery channels as well as the type of clients in their geographic locations. Auditors should have a record of all regulatory requirements in the countries in which the organisation does business. Once all these components have been clearly defined and understood, a risk profile can be developed to ascertain the risk levels and enable drafting of an appropriate audit programme (Khan, 2007: 47).

Shonk (2007a: 8) emphasises that the regulator examiners will evaluate and expect

- independent reviews to verify compliance with the bank's AML policies and procedures
- design and testing of internal controls to prevent money laundering
- a programme that is sufficient in scope
- adequate management
- deficiencies and weakness to be addressed in a timely manner
- how deficiencies are tracked until they are resolved and the adequacy of the tracking system
- that staff conducting the AML programme are accountable to the board.

3.4.2. Who Should be Responsible for Conducting the Review?

US regulations require an independent review, and not a formal audit, to be conducted by a certified public accountant or third-party consultant. Thus, financial services business does not automatically need to hire an outside auditor or consultant. The review may be conducted internally by an officer, employee or group of employees, as long as the reviewer is not the designated compliance officer and

does not report directly to the compliance officer (Department of the Treasury, 2006: 2-3).

Companies may also use qualified internal employees or contract an external auditor to compile a review. However, if an employee conducts the audit they should have solid AML expertise and not be involved in the specific function being tested (Risk Solutions Financial Services, 2007: 8-9).

Compliance monitoring is a continuous process that primarily ensures that business is conducted in accordance with the applicable regulatory requirements and internal audit has a role to play here. In the context of compliance, the role of internal auditing is to ensure that the compliance process is operating effectively (Terblanché et al., 2008).

Beaumier (2005/2006: 31) argues that the responsibility of ensuring the bank's AML programme is effective is a shared responsibility and that the internal auditor or other independent third party is critical to the success of the AML programme.

In the South African context, legislative changes occur regularly and it is important to keep compliance officers updated on the content of the compliance process at all times. The compliance team may either outsource the function or to conduct the review internally at a central point. Generally, the budget of the compliance department determines which choice is taken. The role of internal auditing, given this context, would be to determine if the compliance processes are functioning effectively (Terblanché et al., 2008).

The US Patriot Act is ambiguous as to whether or not an AML audit should be performed by an outside consultant or accountant. What the Act does make clear is that regulators should pay particular attention to the relative independence and competence of individuals performing the audit. Internal auditing should be viewed as a risk management tool designed to identify and correct AML compliance deficiencies prior to any regulatory examination (Shonk, 2007a: 8).

3.4.3. How Often Should a Review Occur?

Compliance officers are required to have a yearly monitoring cycle. This is in line with international best practice for auditors, requiring high-risk areas to be audited every 12 months. In certain instances it might be necessary to monitor specific processes more regularly and this will be based on the risk exposure of the process. There may be a need to ensure continuous compliance in some areas because of significant compliance events or regulatory changes (Terblanché et al., 2008).

The US Department of the Treasury (2006: 2-3) explains that independent reviews should be conducted periodically but the scope and frequency of a review will depend on the business' risk assessment. Risk assessments performed that take the business' products, services, customers and geographic locations into consideration may indicate that an annual review is not necessary or that a more frequent review is be required. For example, if an assessment shows an increase in risk, a more frequent review may be prudent. Likewise, if compliance problems are identified in a review, it may be advisable to move forward the date of the next review to ascertain that appropriate corrective actions have been taken.

Husisian (2010: 29) highlights that it is important that the frequency of the audits vary, depending on the financial institution's risk assessment. Any internal or external testing for compliance should have a scope and frequency proportionate with the risk of money laundering and terrorist financing and in terms of the products and services provided (Anonymous, 2007).

Although there is no guidance provided in the US Patriot Act on the frequency of independent AML programme testing, the regulatory expectation is that independent testing be performed on an annual basis (Beaumier, 2005/2006: 32). In instances where the frequency of the audits is not specified in any statute, a sound practice is to conduct independent testing every 12 to 18 months, depending on the BSA/AML risk profile (Risk Solutions Financial Services, 2007: 9). Shonk (2007a: 8) points out that regulators will examine and assess whether the frequency of audits is suitable for the institution's money laundering and terrorist financing risk.

3.4.4. How should the Review be Documented and Reported to Management?

The person responsible for performing the independent review should document the scope of the review, examine the procedures performed and the transaction testing completed, describe the review findings and give recommendations to management for corrective actions as necessary. Subsequent to the review, the reviewer or the designated compliance officer should track deficiencies and weaknesses identified during the review and document corrective actions. This will confirm that remediate actions were taken to mitigate risks. All relevant documentation should be accessible to government examiners and law enforcement agencies with the authority to examine such documents (Department of the Treasury, 2006: 2-3).

A report containing the audit findings of the AML review should be presented to the board of directors and senior management who will subsequently determine the appropriate course of action (Risk Solutions Financial Services, 2007: 9). Beaumier (2005/2006: 34) argues that the AML audit report should be prepared for applicable legal entities and conveyed to the audit committee comprising primarily of directors with an appropriate understanding of compliance.

3.5. Summary

The fight against money laundering has grown exponentially in recent years, spreading from banks to other financial activities and now into areas that are not necessarily related to finance including company and trust management (Killick & Parody, 2007: 210). This chapter began by providing an overall view of the money laundering dilemma, instances of non-compliance and the high costs associated with mitigating risks (Osborne, 2006: 4)

The second part of the chapter addressed the research topic and considered whether there is a need for independent testing to be performed on AML programmes. Various viewpoints on best practice guidelines are brought to the fore regarding independent testing of AML procedures.

Independent annual audits or other independent forms of testing are viewed as additional safeguards that pre-empt negative regulatory examination findings. The degree of integration within the business, compliance programme and internal audit is often the key to understanding why some AML programmes are effective at mitigating risks and others are not (Axelrod & Ross, 2012: 73). Limitations and challenges have also been identified in terms of independent AML reviews.

Finally, this chapter responds to four critical questions regarding independent AML reviews: what should be done during the AML review, who should perform the review, how often the review should occur and how the review is to be documented and reported to management.

The independent AML review should provide an assessment of the organisation's programme including related policies, procedures, internal controls, record keeping, reporting functions and training (Department of the Treasury, 2006: 2-3). Independent reviews are at the centre of AML compliance and should generally be performed on an annual basis (Beaumier, 2005/2006: 32). It is not clear whether an outside consultant or auditors are needed or not but regulators will pay close attention to the relative independence and competence of individuals performing an AML audits (Shonk, 2007a: 8).

Once all compliance weaknesses have been identified, a report, containing all the audit findings of the AML review, should be presented to the board of directors and senior management who will determine the appropriate course of action (Risk Solutions Financial Services, 2007: 9).

CHAPTER 4

THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS AND OTHER INTERNATIONAL GUIDELINES

4.1. Introduction

A financial crisis engulfed the world in 2007, leaving financial market operators and regulators in turmoil. The magnitude and effects were ubiquitous and alarming. Due to ever-increasing global integration and the complex interconnections between financial institutions, the crisis spread like wild fire across markets and economies (Shehu, 2010: 140).

The crisis highlighted the negative consequences of globalisation and the interconnections between national markets. It exposed illegal investment schemes in complex, financial products that were thought to be reliable, poor corporate governance, inappropriate and ineffective regulatory practices and poor risk management. The financial crisis however provided further momentum to the international AML/CFT cooperation and has led to effective, appropriate regulation (Shehu, 2010: 140).

The fight against money laundering has been an indispensable component in the overall struggle against the illegal trafficking of narcotics and other activities of organised crime (Egmont Group, 2004: 1-2). Combating money laundering is a dynamic process because criminals who launder money are always seeking new ways to achieve their illegal ends. They also seek to exploit weaknesses in other non-financial industries in order to continue their laundering activities (FATF, 2003a: 3). Perpetrators have demonstrated adaptability by finding new means to launder the proceeds of illegal activities (FATF, 2009a: 5).

The globalisation of financial markets and rapid information technology changes have boosted the criminal economy and expanded possibilities for economic crimes. There is an alarming and growing concern over the range of legitimate business sectors in danger of being contaminated by criminal money (FATF, 2009a: 5).

With the increase in globalisation and liberalisation of financial systems, countries have become more susceptible to money laundering and its detrimental effects. The scale of money laundering and the damage it causes led to national and international strategies to control the problem (Commonwealth Secretariat, 2006: 17-21).

Since the 2001 terrorist attacks in the US, money laundering and the financing of terrorism have been expressly being linked. The financial system became an essential component in the fight against money laundering and terrorist financing. Initially the fight was against laundering profits from the illegal drug trade buts now it seeks to uproot the flow of terrorist funds and the reasoning was to starve the funds of terrorism so they cannot carry out destructive campaigns (Johnson, 2008: 7).

Money laundering is a type of criminal activity with no borders or boundaries. The fight against money laundering is global with various treaties and agreements being made between countries. One of the key agreements that guide the fight against money laundering is the FATF Forty Recommendations (Yasin, 2004: 364). A number of government agencies have been created and are commonly known as financial intelligence units (FIUs). These units have an important role in AML programmes (Egmont Group, 2004: 2).

4.2. The Financial Action Task Force

4.2.1. The Origins and Background of the FATF

In response to the concerns over money laundering, the G-7 Summit in Paris in 1989 established the Financial Action Task Force (FATF) as an inter-governmental body. After recognising the threat money laundering posed to the banking system and financial institutions, the G-7 leaders assembled the Task Force from the G-7 member states, the European Commission and eight other countries (FATF, 2010b).

Initially, the FATF mainly focused on money laundering from drug trafficking but later expanded their mandate to money laundering in general and later to terrorist financing (Jakobi, 2012: 22). As a result of the change in focus, organisations that

were originally set up with an AML focus now include procedures for countering the financing of terrorism (Johnson, 2008: 7).

The FATF pursues three main objectives: to strengthen anti-criminal law by improving national legal systems regarding money laundering, to increase global AML cooperation and to develop the role of the private sector in fighting money laundering (Jakobi, 2012: 22).

Other FATF key objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats posed to the integrity of the international financial system. The FATF is therefore seen as a "policy-making body" focusing on bringing about national legislative and regulatory reforms (FATF, 2010b).

In order to execute its mandate, the Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national and international level and identifying measures that still needed to be put in place to combat money laundering (FATF, 2010b).

4.2.2. FATF Membership

In 2008, the FATF standards were endorsed by more than 170 countries around the world including the International Monetary Fund (IMF) and the World Bank. The FAFT gives recommendations for combating money laundering and terrorist financing and encourages its members to practice them by way of a mutual evaluation process (Ping, 2008: 321). In addition, the endorsement of the FATF standards by 170 countries that represent more than 85% of the world, confirms the extent of its compliance recommendations (Beekarry, 2011: 174).

The FAFT has 34 states and two regional organisations as members. The regional organisations are the European Commission and the Gulf Co-operation Council. South Africa joined the FATF in June 2003 (De Koker, 2012: 1-13).

Other noteworthy initiatives include the formation of eight regional bodies with essentially the same AML/CFT objectives as the FATF. The eight organisations are

the Caribbean Financial Action Task Force, the Eurasian Group, the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), the Intergovernmental Action Group against Money laundering in Africa (GIABA), the Asia/Pacific Group on Money Laundering (APG), the FATF of South America Against Money Laundering (GAFISUD), The Middle East and North Africa Financial Action Task Force (MENAFATF) and the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures. These groups were set-up to counter money laundering and terrorist financing by tailoring AML/CFT recommendations to their local environment (Johnson, 2008: 7, 9, 10).

4.2.3. The FATF Recommendations

In April 1990, the FATF introduced the 40 Recommendations on money laundering. The Recommendations were revised in 1996 and 2003 to reflect changes in patterns in money laundering and are now recognised as international standards in combating money laundering (Gardner, 2007: 329).

The FATF 40 Recommendations were drawn up as an initiative to combat the misuse of financial systems by persons laundering illegal drug money. The Recommendations provided the necessary comprehensive plan of action to fight money laundering. In 1996 the Recommendations were revised to reflect evolving money-laundering trends and techniques and to extend their scope beyond illegal drug-money laundering. In October 2001 the FATF further expanded its mandate to deal with the funding of terrorist acts and terrorist organisations by creating the Eight Special Recommendations on Terrorist Financing (FATF, 2012: 7).

The FATF Recommendations are meant to be the minimum standards enabling countries to implement the requirements based on the circumstances and constitutional framework of each country. The recommendations recognise that countries have different legal and financial systems and that they cannot all use the same measures to achieve the common purpose (Jensen & Png, 2011: 113).

The recommendations give an outline for developing a complete set of AML measures and guidelines that cover the relevant laws and their enforcement, the

activities and regulations of the financial system and matters concerning international cooperation (Johnson, 2008: 11). Leong (2007: 148) says that the 40 Recommendations provide a comprehensive AML blueprint for improving national systems, establishing the role of financial systems and facilitating international cooperation.

The FATF standards allow countries a measure of flexibility in implementing the principles, according to their unique circumstances and constitutional frameworks (Shehu, 2010: 142). Gardner (2007: 33) states that the 40 Recommendations set-out a comprehensive framework and global application and, even though there was no binding international commitment by the international community, a large number of countries have a political commitment to implement the plans.

According to Shehu (2010: 142) the recommendations have been recognised, endorsed and adopted by over 182 countries that have made a firm political commitment to AML/CFT by implementing the FATF standards.

In October 2004, the FATF published the Ninth Special Recommendation, further intensifying international AML/CFT standards (FATF, 2010b). The FATF 40 + 9 Recommendations provide a complete set of counter-measures for AML/CFT covering the criminal justice system, law enforcement, the financial system and its regulations and international co-operation (Shehu, 2010: 142).

The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have now been endorsed by over 180 countries (FATF, 2012: 7). Following mutual evaluations of its members, the FATF standards have been revised and updated a third time. Accordingly, the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (The New FATF Recommendations) were released in February 2012 (FATF, 2012: 7).

The FATF Recommendations (2012: 7) set out the crucial measures that countries should have in place to identify risks; develop policies and domestic coordination; pursue money laundering, terrorist financing and the financing of proliferation; apply

preventive measures for the financial sector and other designated sectors; establish powers and responsibilities for the competent authorities (e.g. investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and facilitate international cooperation (FATF, 2012: 7).

The internationally endorsed global standards for implementing effective AML/CFT measures have increased the transparency of the financial system and given countries the capacity to act against money launderers and terrorist financiers in an effective manner (FATF, 2010: 2).

The FATF not only puts forward recommendations to establish international standards for AML but also encourages members to implement them in practice by way of an evaluation process (Ping, 2008: 321). Through annual self-assessment, the FATF regularly reviews its members to check compliance with the Recommendations identifies emerging trends and methods used to launder money and suggests measures to combat them (FATF, 2003a: 3).

4.2.4. The FATF Recommendations on Independent AML Reviews

The FAFT 40 Recommendations published in 2003 require that financial institutions to develop internal policies, procedures and controls supported by appropriate compliance management and an audit function to test the systems (FATF, 2003b: i).

An omission in the earlier versions was identified: the Recommendations were not explicit on the need for independent reviews of AML controls. Independent reviews did not feature explicitly in the FATF 40 + 9 Recommendations either which simply requires financial institutions to have appropriate policies and procedures for “internal control” (FATF, 2012: 77).

The recommendations did highlight let alone suggest independent as an AML priority (Delston, 2007: 6). On the other hand, in 2007, the FATF released guidance notes as an additional measure, primarily addressing public authorities and financial

institutions. The guidelines advocated the use of a risk-based approach to money laundering (FATF, 2007: 2).

By adopting a risk-based approach, the FATF (2007: 2) argues that knowledgeable authorities and financial institutions are able to ensure that proportionate measures are in place to prevent or mitigate money laundering and terrorist financing. It is through this process that financial institutions are better able to recognise the existence of the risk(s), assess the risk(s) and develop strategies to manage and mitigate the identified risk(s).

Through the guidance notes, the FATF (2007: 29) pointed out that senior management will need to independently validate the development and operation of the risk assessment management processes and related internal controls to obtain adequate assurance that the risk-based methodology in use accurately reflects the financial institution's risk profile.

This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not necessarily involved in the implementation or operation of the financial institution's AML/CFT compliance programme (FATF, 2007: 29).

In February 2012, the FATF released the New FATF Recommendations. Like the earlier guidelines released in 2007, the latest standards emphasise the need for a risk-based approach to money laundering to ensure that risks are mitigated effectively (FATF, 2012: 11).

According to the FATF (2012: 78), financial institution programmes against money laundering and terrorist financing should at least include

- the development of internal policies, procedures and controls
- appropriate compliance management arrangements
- adequate screening procedures to ensure high standards when hiring employees

- an ongoing employee training programme
- an independent audit function to test the system.

Following mutual member evaluations, the FATF standards have been revised and updated to improve the requirements whereby an independent audit function to test the system has now been incorporated as an AML priority (FATF, 2012: 8, 77).

One shortfall noted is that although the latest FATF Recommendations identify independent reviews as an AML priority, they do not explicitly state who should perform these independent reviews. The necessary skills, qualifications and experience of the person performing the independent AML reviews are also not described.

4.3. The UK Anti-money Laundering Measures

4.3.1. Background to the UK AML Regime

The British economy is one of the most open in the world. In international finance, the City of London exports £19 billion more in financial services than it imports. Yet the opportunities of globalisation can also be used to do harm, as well as good. Sophisticated criminal and terrorist networks have emerged that are both entrepreneurial and international. These now pose a significant challenge to the UK at home and abroad (HM Treasury, 2007: 5).

Sproat (2009: 135) emphasises that organised crime in Britain is one of the most serious forms, generating large amounts of profit annually. A substantial amount of this money is laundered through a regulated financial sector.

The UK plays a critical part in deciding and promoting AML/CFT strategies, given the role of London as a major international financial centre. The AML strategy in the UK involves mainly criminal, civil and regulatory law (Leong, 2007: 141-142).

The initial three main constituents in the UK legislative and regulatory framework were: the government, which sponsored legislation, defined criminal offences and drafted money laundering regulations; the Financial Services Authority (FSA) which

was mainly in charge of making regulatory rules to counter money laundering; and the Joint Money Laundering Steering Group (JMLSG) which issued comprehensive guidance notes on the meaning and application of regulations and best practice (Leong, 2007: 141-142).

In April 1 2013, the U.K. moved towards the "twin peaks" model of financial regulation. This model saw the Financial Services Authority cease to exist and its work split between two new regulatory authorities, specifically the Prudential Regulation Authority and the Financial Conduct Authority which will now regulate the conduct of financial institutions (Stikeman, 2013).

In the UK there are numerous regulatory bodies besides the FSA (now known as the FCA) that address financial services activities, namely the Pension Regulator and The Takeover Panel. There are also a number of laws and regulatory bodies that govern the national AML effort (Mills, 2008: 3).

Given the immense scale of money laundering, the UK implemented its own AML/CFT legislation and numerous industry guidance notes have been drafted and circulated to limit and reduce the dilemma. The most significant is the JMLSG Guidance Notes (Mills, 2008: 11).

The UK's approach to fighting money laundering and terrorist financing relies on a partnership between the public and private sectors. Key objectives are specified in legislation and in the FSA Rules, but these do not prescribe how these objectives must be met (JMLSG, 2011: 21).

The objectives are rather a requirement of the EU Directive, incorporated into UK law without any further expansion. UK financial business may use their own discretion in the interpreting of how the objectives should be met. Key elements of the UK AML/CTF framework are the

- Proceeds of Crime Act of 2002 (as amended)
- Terrorism Act of 2000 (as amended by the Anti-terrorism, Crime and Security Act of 2001)

- Money Laundering Regulations of 2007
- Counter-terrorism Act of 2008, Schedule 7
- HM Treasury Sanctions Notices and News Releases
- FSA Handbook
- implementation of guidance for the financial services industry as provided by the JMLSG (JMLSG, 2011: 21).

Requirements are also enforced by supervisors such as the FSA. These use a risk-based method. The bodies promote strict adherence and require financial institutions to have suitable systems of internal controls in place to reduce the opportunities for financial abuse (HM Treasury, 2007: 20).

4.3.2. Financial Services Authority

The Financial Services Authority (FSA) is the financial regulator for the UK, serving as an independent supervisory body accountable to the Treasury and Parliament. The FSA was formed in May 1997 and its key objectives pertaining to money laundering are to reduce the extent to which it is possible for a firm to be used for a purpose connected with financial crime including money-laundering (FSA, 2012).

The FSA has taken over the responsibilities of nine regulators and plays a major part in UK legislative and regulatory framework with regard to money laundering. The FSA has been vested with powers of supervision and enforcement. It imposes five main duties under the Money Laundering Regulations (MLR): know your customer, record keeping procedures, establish a Money Laundering Reporting Officer (MLRO) to ensure that suspicious activities are reported internal and externally and to impose internal controls to prevent money laundering (Leong, 2007: 144).

The FSA also promotes the adoption of a risk-based approach to money laundering emphasising that resourcing be allocated on a proportionate basis in relation to the risk faced by financial institutions (Leong, 2007: 144).

4.3.3. Joint Money Laundering Steering Group

The Joint Money Laundering Steering Group (JMLSG) consists of 16 leading UK Trade Associations in the financial services industry whose purpose is to provide practical assistance and guidance in interpreting the MLR (Leong, 2007: 144).

The group is a private sector body which provides an authoritative account of how high-level requirements of the MLR can best be applied in specific sectors, with the aim of promulgating good practice in countering money laundering and to give practical assistance in interpreting the UK MLR (JMLSG, 2012). Through the use of the JMLSG Guidance Notes courts can determine whether there has been a breach of the MLR and if there are reasonable grounds for suspicion of money laundering (Leong, 2007: 144).

These JMLSG Guidance Notes provide comprehensive direction on two main levels: the internal AML infrastructure that financial services should implement (staff training, identifying and reporting suspicious of money laundering) and the actual "know you customer" KYC checks that financial institutions should carry out when dealing with particular types of customers and transactions. The guidance, prepared by the JMLSG, is addressed to financial institutions in the industry sectors represented by its member bodies and to those financial institutions regulated by the FSA. All such financial institutions should have regard for the contents of the Guidance Notes and include those that are members of the JMLSG trade associations but not regulated by the FSA and those regulated by the FSA that are not members of the JMLSG trade associations. (JMLSG, 2011: 9).

4.3.4. UK Measures for AML Compliance and Independent AML Reviews

Consistent with the views raised by the FATF, the UK guidelines emphasise the responsibility of senior management in managing the firm's money laundering and terrorist financing risks using a risk-based approach (JMLSG, 2011: 10).

According to the JMLSG (2011: 20), senior management must be fully engaged in the decision-making processes, take ownership of the risk-based approach and be held accountable if the approach is inadequate. Senior management must be aware

of the level of money laundering risk exposure and determine whether the firm is adequately equipped to mitigate that risk effectively.

In following the risk-based approach, management should summarise how the approach might be established by

- identifying and assessing the risks faced by the firm
- designing and implementing controls to manage and mitigate the risks
- monitoring and improving the effectiveness of the firm's controls
- recording the actions taken and why
- noting that risk management is generally a dynamic, continuous process rather than a one-time exercise (JMLSG, 2011: 14).

The position in the UK is rather interesting. The principle of annual review is contained in the FSA rules. The rules highlight that it is the MLRO, not the independent party, who must report, at least annually, on the operation and effectiveness of the AML system and controls. The FSA rules place the onus on the institution itself to carry out regular assessment to ensure their compliance to set rules. The JMLSG guidance contains no recommendations on independent reviewing (Delston, 2007: 6).

4.4. The European Union Anti-money Laundering Measures

4.4.1. Background of the EU AML Systems

Over the past two decades the European Union has emerged as a leader in financial sanctions and has created a successful AML regime as well as an effective framework to combat the financing of terrorism. The origins of the EU AML/CFT regime can be traced back to the late 1980s when organised crime and money laundering required new and innovative responses (Ganguli, 2010: 1).

In September 1990, a new Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime was adopted by the Committee of Ministers of the Council of Europe. The convention dealt with all types of crimes and went beyond the Vienna Convention. The offence of money laundering was extended to

all associated serious criminal offences. This was a pivotal change as it was now realised that criminal syndicates did not specialise in one product alone and that money laundering was highly complex (Commonwealth Secretariat, 2006: 19).

4.4.2. EU AML Directives

The EU became actively involved in the fight against money laundering in the early 1990s with a Directive aimed at the prevention of the use of the financial system for the purpose of money laundering (the First Directive) released in 1991. The Directive was later amended by the Second Directive released in 2001, which, among other things, broadened the scope of the First Directive to include non-financial institutions such as notaries and lawyers et cetera. In response to the revision of the FATF Recommendations, the Third Directive was introduced in 2005 as an improvement to the Second Directive. Its primary objective is to provide a common basis for implementing the FATF Recommendations in the EU (Van den Broek, 2011: 170).

The Third EU AML Directive is a key element in the EU response to money laundering and international terrorism and intends to modernise the legal framework in the EU in accordance with existing international standards, in particular, the revised FATF Recommendations of June 2003. The adoption of the Third EU AML Directive has led to the rise of a new and effective AML/CFT regime in Europe (Ganguli, 2010: 2).

These include “customer due diligence” (CDD) processes, “Know your Customer” (KYC) policies, risk-based identification, business relationships with politically exposed persons (PEPs) and the application of AML/CFT measures (Ganguli, 2010: 2). Consistent with the view raised by Ganguli, O’Reilly (2006: 59) highlights that the Third EU AML Directive was a significant improvement to the previous two Directives and introduced improved KYC duties and additional scrutiny of PEPs.

The aims and objectives of the EU legal regime on AML are largely borrowed from the FATF. The legal formulation of the relevant rules in the EU AML Directives appears to be more or less a verbatim copy of the FATF Recommendations. The key

distinction is that the EU AML regime is a more effective method of implementation and enforcement of the rules (Seyad, 2012: 34).

A dual approach was developed by the EU consisting of a preventive policy, which aimed at hindering money laundering through identification and reporting obligations, and a repressive policy, aimed at punishing money launderers (Van den Broek, 2011: 170).

4.4.3. EU Directives on Independent AML Reviews

Historically, European AML policy takes a preventative stance which involves protecting the financial system from money laundering. The foundation of the European system remains the Third Anti-Money Laundering Directive adopted in 2005 (Tavares, Thomas, & Roudaut, 2010: 5).

Seyad (2012: 40) argues that the later AML Directives and amendments released aimed at rectifying the shortcoming of the previous Directives. The First Directive only covered illegal drug trafficking as a cause of money laundering while the Second Directive expanded its scope to include other avenues of money laundering but the Directives were still inadequate. The Third Directive however also have a number of drawbacks that prevent effective AML/CFT.

When the Euro was introduced in 1999 as a single currency for the majority of the EU member states the First Directive was seen as inadequate to deal with the potential abuse of the new currency in the EU financial market. The Directive had certain inherent limitations and in order to ensure that the Euro is not exploited by criminals as a vehicle for money laundering, the EU decided to update and amend the First Directive (Mohamed, 2002: 66).

Another drawback of the First Directive was the narrow definition of financial institutions. Certain financial institutions were not specifically covered. The Directive defined money laundering in terms of property rights which was inadequate and left much leeway for member states. The First Directive also lacked uniformity regarding

the nature and form of sanctions to be imposed for breaching the Directive (Mohamed, 2002: 66).

Seyad (2012: 40) states that the Directives are based on the principle of harmonisation and that the integrated model is appropriate and sufficient for the different financial sectors such as the banking and investment services but has proved to be inadequate to deal with the greater corruption and terrorist financing problems in the financial market. Another pivotal issue was the competence of EU criminal law.

However, the Third Directive was an improvement on the previous AML Directives. The Third Directive extends EU law to cover terrorist financing and requires that regulated persons promptly furnish the FIU with all necessary information (O'Reilly, 2006: 59).

In addition, the Third Directive pays attention to the enforcement of preventative AML/CFT policies. Supervision takes centre stage with supervisory authorities obliged to monitor whether all requirements from the Third Directive, particularly the CDD measures, reporting obligations and record keeping measures, are adhered to. The Directives clearly state that supervisory authorities must always be able to effectively monitor compliance, have adequate powers to do so, perform checks and have sufficient resources to perform their supervisory functions (Van den Broek, 2011: 177).

Independent audits do not feature in the Third or earlier Directives. The Directives simply require that financial institutions have appropriate policies and procedures for “internal controls”. The word “appropriate” may perhaps be interpreted to encompass independent reviews; however, the Directives do not explicitly identify independent reviews as a priority (Delston, 2007: 6).

It is reasonably concluded that the Third Directive pays more attention to supervision and sanctioning than the earlier Directives and imposes various minimum standards which enforcers must meet (Van den Broek, 2011: 178).

4.5. US Anti-Money Laundering MEASURES

4.5.1. Background to AML in the US

The size and significance of the US economy, its sophisticated banking systems and the fact that the two largest stock exchanges NASDAQ and NYSE are based in the US contribute to its importance in the global arena and particularly in relation to the development of the AML concept (Pieth & Aiolfi, 2002: 25).

The history of US AML legislation began with the 1970 Bank Secrecy Act (BSA) which was passed because of concerns over the susceptibility of financial institutions to organised crime, particularly those linked to narcotics trafficking. Due to the escalating volume, scope and complexity of money laundering activities in the 1980s and 1990s another six AML regulations were passed (Dollar & Shughart, 2011: 20).

US AML laws and regulations for financial institutions are not new developments. These laws have raised compliance requirements for financial institutions. The US Government devotes a large amount of resources to AML and enforces sanctions and penalties. This is evidenced by the recent US$350 million fine imposed of Lloyds TSB Bank Plc. for funds laundered through the bank from countries and entities under sanctions (Husisian, 2010: 14).

4.5.2. The US Patriot Act of 2001

Following the terrorist attacks in September 2001, Congress passed the US Patriot Act providing appropriate tools for intercepting terrorists. The Act was signed into law in October 2001. Its main purpose is to deter and punish terrorist acts in the US and around the world and to enhance law enforcement investigation tools (Risk Solutions Financial Services, 2007: 2).

The 9/11 terrorist attacks, USA Patriot Act and other legislative responses to terrorist attacks set off a remarkable change in the fight against money laundering in the rest of the world (Dollar & Shughart, 2011: 20). The enactment of the US Patriot Act was

a direct response to terrorist activities in 2001. The Act's main purpose is to enhance the prevention, detection and prosecution of international money laundering and terrorist financing (Beaumier & Shah, 2003: 13).

Title III of the Patriot Act for the most part impacts financial institutions and addresses terrorist financing and money laundering by expanding existing AML laws, primarily the BSA. It defines a "financial institution" broadly so that the scope of money laundering regulations now applies not only to traditional financial institutions (such as banks, thrifts, savings and loans) but to non-financial institutions as well (Risk Solutions Financial Services, 2007: 2).

The AML standards apply to a broad range of institutions and introduce additional measures such as enhanced due diligence (EDD) for correspondent and private banking accounts and customer information programmes (Beaumier & Shah, 2003: 13).

4.5.3. The USA Patriot Act on Independent AML Reviews

The Patriot Act of 2001 is one of the most comprehensive counter-terrorist laws passed after the 9/11 events. Title III of the Patriot Act transformed US money laundering laws for the purpose of disrupting financial networks that support terrorist organisations and was considered the most extensive AML laws ever passed by the US (Dollar & Shugart, 2012: 127).

The Patriot Act requirements are built on existing standards and guidelines published by global organisations and are widely adopted as best practice standards. The practices mandated by the Act are not necessarily new. However, for organisations that were not formerly subject to BSA requirements, particularly the non-banking financial institutions, the application of AML standards to these industries are undeniably new (Risk Solutions Financial Services, 2007: 2).

Title III of the US Patriot Act is also commonly known as the International Money Laundering Abatement and Financial Act (Terrorism Act) of 2001 which have

strengthened the existing AML regulations. The 2001 laws expanded the narrow focal point of money laundering to encompass terrorist financing and further increased the number of financial and non-financial institutions subject to AML laws. The laws went further by introducing requirements that are not only national but international in their scope and application (Dollar & Shughart, 2011: 20).

The new provisions require new AML elements and due diligence standards. Financial institutions are now expected to conduct a thorough risk analysis and develop policies and procedures that effectively address the risks identified (Risk Solutions Financial Services, 2007: 2).

To guard against money laundering through financial institutions the US Patriot Act requires that each financial institution establish AML programs, including, at a minimum, the development of internal policies, procedures, and controls; the designation of a compliance officer; an ongoing employee training programme; and an independent audit function to test programmes (US Government, 2001: 322).

According to Axelrod and Ross (2012: 72), the US Patriot Act requires personnel inside and outside an institution to carry out annual independent tests of the AML programme. Internal auditing is generally considered to have sufficient independence to perform this role.
Although compliance testing is a vital part of the framework, the compliance department, which is typically responsible for the policies and procedures being tested and evaluated, is generally not considered adequately independent for the purposes of the Patriot Act. Often, internal auditors conduct the independent test and compliance officers carry out additional testing. Internal auditors may use the results of the compliance tests in planning their independent tests (Axelrod & Ross, 2012: 72).

AML audits aim to test a financial institution's adherence to its compliance programme and to its regulatory responsibilities. Auditors are therefore required to use a risk-based approach that is centred on the areas where issues are likely to

arise. One such area that requires special attention in financial institutions involves performing sanctioned compliance audits (Husisian, 2010: 14, 22).

Based on the views provided, we can make reasonable the assumption that AML reviews are an integral part of the US regime but it is also critical that these reviews are performed by an independent auditing function.

4.6. Summary

This chapter gives an overall view of money laundering. Money laundering is a challenge. The context was provided to ascertain the extent of money laundering globally. Money laundering is a serious worldwide threat. Countries are flooded with illicit funds and vulnerable to the breakdown of the rule of law (US State Bureau for International Narcotics and Law Enforcement Affairs, 2012: 3).

Money laundering methods and techniques change in response to developing counter-measures. The escalation of money laundering has been a worldwide concern and a multi-faceted global predicament. The FATF has noted the increasingly sophisticated combinations of techniques including the increased use of legal persons to disguise the true ownership and control of illegal proceeds and the use of professionals to provide instruction and assistance for laundering criminal funds (FATF, 2003b: i).

In response to the problem, AML is viewed as a global concern which saw the inception of the Financial Action Task Force and other international bodies (Egmont Group, 2004: 1-2). This chapter provides an overview of the FATF and other AML guidelines. To provide a sound comparison on best practice, four main guidelines were assessed, namely, the FATF recommendations, the EU Directives, the US Patriot Act and the UK money laundering regime.

Background to each of these regimes was provided to show how they came about, why they exist and, most importantly, to support the research conclusions much focus was paid to their views on independent AML reviews. This chapter provides a

balanced literature review with particular reference to independent AML compliance from an impartial viewpoint.

The New FATF Recommendations require an independent audit function to test AML systems and this has now been incorporated as an AML priority (FATF, 2012: 8 & 77). The position in the UK emphasises that it is the MLRO, not the independent party, who has to report at least annually on the operation and effectiveness of the AML system and controls. The FSA perspective highlights that the JMLSG guidance contains no recommendations on independent reviews (Delston, 2007: 6).

Independent audits do not feature in the EU Third Directive. The requirement is that financial institutions have appropriate policies and procedures for "internal controls". The Directives do not explicitly suggest independent reviews as a priority (Delston, 2007: 6). Through the USA Patriot Act of 2001, the US requirement is that independent audits are a pivotal part of an AML programme and the personnel inside or outside an institution should carry out annual independent tests of the AML programme (Axelrod & Ross, 2012: 72).

It is clear that in some regimes independent AML reviews form an integral part of the preventative programme while in others this is not a priority. The South African AML measures will be discussed in detail in chapter 5. Chapter 5 looks at South Africa's AML regime and provides a comparative view in relation to global regimes.

CHAPTER 5

MONEY LAUNDERING AND ANTI-MONEY LAUNDERING MEASURES IN SOUTH AFRICA

5.1. Introduction

5.1.1. Background and Context of the South African Money Laundering Problem

The Republic of South Africa is a developing country occupying the southern part of the African continent. The country has a surface area of 1 219 million kilometres with common boundaries with Botswana, Mozambique, Namibia, Swaziland and Zimbabwe. South Africa has an estimated population of 47,9 million (FATF, 2009b: 14).

South Africa is a regional financial centre with a modern financial system and banking infrastructure. There are a number of banks with branches operating in South Africa and some are locally controlled while others are part of international organisations. In addition, South Africa has an exchange control regime, with currency exchange being conducted by authorised dealers in foreign exchange appointed by the Minister of Finance and regulated by the Exchange Control Department (EXCON) of the South African Reserve Bank (SARB) (IMF, 2004: 1).

South Africa's economy remains primarily cash-based although it has a first-world banking sector characterised by a well-established infrastructure and technology and there is a growing demand for financial services. As a matter of priority, the government, in partnership with local banks, endeavours to ensure that individuals currently excluded from using formal financial services, particularly potential low-income customers, can have access to them. Registered financial services providers now offer services in line with this need (FATF, 2009b: 6).

Commercial crimes primarily affect the banking and business sectors. A study conducted by Pricewaterhouse Coopers (PwC) in 2007 suggested that South Africa is mostly affected by economic crimes such as asset misappropriation, money laundering, bribery and fraud (Hübschle, 2010: 69).

As a semi-developed financial system, South Africa offers a range of products that criminals can easily use to launder their illicitly obtained money. The products on offer range from internet banking facilities and off-shore unit trust investments to small savings accounts that target individuals with little or no access to banking services previously and criminals are taking full advantage of the system (De Koker, 2002a: 13).

According to De Koker (2002a: 13-14), a significant amount of illegal funds are deposited into customer bank accounts. Criminals may deposit money into their own bank accounts but more sophisticated criminals often open accounts with false identification documentation. Alternatively, criminals open an account in the name of a front company or trust. In more complex schemes, criminals use credit and debit card facilities to launder money and to move proceeds of crime across the borders of South Africa. There is also an identified pattern in which legitimate bank accounts of family members or other related third parties are used.

Illicit financial flows constitute a significant problem in the African continent. The methods used vary and include tax havens and secrecy jurisdictions, over-invoicing and under-pricing and other different money laundering strategies. These methods are greater in scale than the commonly used corruption channels (Goredema, 2012).

Nevin (2000: 20) points out that Africa is rapidly becoming a “washing machine” for organised crime. Many communities still prefer to keep their funds in notes and coins rather than using banks. This financial environment creates an excellent opportunity for the money launder.

5.1.2. The Financial Impact and Implications of Money Laundering in South Africa

Money laundering has not only negatively impacted the economies of African countries, but it has also seriously damaged the international image of the continent. In Africa, the problem of money laundering discourages legitimate business and foreign direct investment, corrupts the financial system and eventually the socio-political systems as well (Okogbule, 2007: 449-450).

In the South African criminal law context, the term “money laundering” refers to a number of different offences that can be committed in terms of the Prevention of Organised Crime Act No. 121 of 1998 (POCA). The concept overlaps with certain common law offences (i.e. fraud, forgery and uttering) and statutory offences (i.e. corruption) (De Koker, 2002a: 27).

Common schemes include fraud, theft, corruption, racketeering, precious metal smuggling, abalone poaching, “Nigerian-type” economic and investment frauds and pyramid schemes. There are an increasing number of complex, large-scale economic criminal syndicates. South Africa is also a transport route for drug trafficking (FATF, 2009b: 6).

It is not precisely known how much money is laundered nationally and internationally. The FATF attempted a project to estimate the value of laundered funds in the 1990s but the project was abandoned when it became clear that the study would not be able to produce reliable results (De Koker, 2012: Com 1-4). This indicates that accurately measuring money laundering is a complex and difficult process.

Although the level of laundering in the informal economy cannot be measured with certainty, in all probability, it is quite substantial (De Koker, 2002a: 13-14). The amount of the money flowing through global financial systems is huge and has a massive impact on a country’s economy, government and social well-being (FIC, 2006/2007: 10).

Moshi (2007: 2) states that the amount of illicit funds generated through organised crime is substantial and there is a wide-ranging abuse of informal banking, financing channels and alternative remittance systems to an extent that the informal systems operate outside the regulated system.

In South Africa in 2009 and 2010 the FIC reported that R 66.1 billion is the suspected estimate of the proceeds of crime and money laundering. These funds represent real losses for a developing economy (FIC, 2010/2011: 6).

According to the Task Force on Financial Integrity and Economic Development, every year developing countries lose roughly US$1,3 trillion in illicit financial flows including the proceeds of crime, corruption, tax evasion and trade mispricing (FIC, 2011/2012: 10).

For many years, criminals have been taking steps to hide the true nature of their proceeds but law enforcement agencies began paying close attention to the flow of criminal funds and money laundering control has become a new strategy for combating crime and terrorism. The changes were radical with a new regulatory system developed which forged a crime combating relationship between law enforcers and financial institutions (De Koker, 2012: Com 2-3).

Governments around the world, including South Africa, recognised the urgency and importance of fighting money laundering. The South African government introduced comprehensive AML legislation in the form of the Financial Intelligence Centre Act effective from February 2002 (Cromhout, 2002: 5).

In the 2013 budget speech, the Minister of Finance Pravin Gordhan told Parliament that worldwide, special measures are being taken to oversee the accounts of those who have become known as politically exposed persons (PEPs), including public representatives and senior officials. A special request was also made to the FIC to explore alternatives for bringing South Africa into line regarding international anti-corruption and AML standards (South African National Treasury, 2013: 29).

5.2. South African AML Measures

5.2.1. Background to AML Laws and Regulations in South Africa

In describing the journey the FIC has travelled the previous Minister of Finance, Trevor Manuel, told Parliament that:

> Money launderers view the financial system as a device to transfer the proceeds of their crime and to legitimise their activities. When they involve the financial system in money laundering schemes, they

> necessarily involve institutions that provide access to system... It can result in erosion of public confidence of our financial institutions and undermine the stability of the system. If financial institutions are indifferent to this it may cause them to suffer losses through fraud and effects of being associated with criminals. None of us, not the banks, not ordinary citizens – want this to happen (FIC, 2006/2007: 3).

South Africa's AML/CFT regime comprises a three-tier framework: legislation, regulations and sector-specific guidelines (Goredema, 2007: 77). Since the early 1990s, South Africa has developed a comprehensive legal framework to fight money laundering and terrorist financing. The first statutory provisions that addressed money laundering were outlined in the Drugs and Drug Trafficking Act No. 140 of 1992. These are viewed as the first generation of statutory AML provisions in South African law that focus on drug-related offences. The second generation of money laundering provisions was introduced by the Proceeds of Crime Act No. 76 of 1996, broadening the scope of AML provisions to include the proceeds of any offence. The third generation laws were introduced by the Prevention of Organised Crime Act No. 121 of 1998 and the Financial Intelligent Centre Act No. 38 of 2001 (De Koker, 2012: Com 2-3).

The main AML/CFT laws are the Prevention of Organised Crime Act No. 121 of 1998 (POCA), the Protection of Constitutional Democracy against Terrorist and Related Activities Act No. 33 of 2004 (POCDATARA) and the Financial Intelligence Centre Act No. 38 of 2001 (FICA). Generally, these laws are aimed at transactions involving the proceeds of unlawful activities or that are aimed at financing terrorist and related activities. The Acts also created compliance obligations for businesses and their employees (IRBA, 2011: 3-4).

In order to combat money laundering activities and terrorist financing in South Africa the Financial Intelligence Centre was also established under the FIC Act No. 38 of 2001, abbreviated to "FIC". The FIC has mainly four AML pillars to combat money laundering and terrorist financing namely, the establishment and verification of

identity, record keeping, client profiling and reporting of suspicions and unusual transactions (FIC, 2006).

The FIC Act also broadened the scope of money laundering control duties of businesses to include combating the financing of terrorism. The provisions were wider in their reach and more detailed than the previous laws. They created a comprehensive set of money laundering control duties for accountable institutions and brought forth compliance obligations for financial institutions and other businesses (De Koker, 2012: Com 2-3).

5.3. AML Laws and Regulations in South Africa

5.3.1. The Drugs and Drug Trafficking Act No. 140 of 1992

The Drugs and Drug Trafficking Act No. 140 of 1992 is the first set of provisions that dealt explicitly with money laundering. The Act criminalised money laundering proceeds related to specific drug-related offences and required the reporting of suspicious transactions involving the proceeds of drug-related offences (De Koker, 2012: Com 2-4). De Koker (2012: Com 2-4) argues that although the money laundering provisions look impressive, in practice they have a very limited effect because the confiscation procedure is rarely used. Likewise, reporting in terms of the Act has not been satisfactory and the scope has been limited to the proceeds of drug-related offences only.

5.3.2. The Proceeds of Crime Act No. 76 of 1996

To address international cooperation in criminal prosecutions regarding money laundering, the Proceeds of Crime Act No. 76 of 1996 was enacted. The Act criminalised the laundering of proceeds of any type of offence and created a reporting obligation for businesses that come into possession of any suspicious property. It allowed for the freezing of assets and the confiscation of criminal proceeds. Though the relevance of this Act is decreasing, core aspects may still be important in certain cases (De Koker, 2012: Com 2-6).

5.3.3. The Prevention of Organised Crime Act No. 12 of 2004 (POCA)

Due to the rapid growth of organised crime in South Africa and the failure of statutory law to keep pace with international measures the POCA was adopted (Kruger, 2008: 5). Kruger (2008: 5) argues that conventional criminal law procedures and penalties were inadequate to combat and deter organised crime, and further highlights that, internationally there was a common thought that criminals should be stripped of proceeds of crime in order to remove the incentive of crime.

In 1998, the South African government decided to take a stronger stand against organised crime by drafting and adopting the Prevention of Organised Crime Act No. 121 of 1998 effective from 21 January 1999, commonly known as the POCA. In addressing the scourge of money laundering, the POCA criminalised certain activities linked to racketeering and described offences related to the activities of criminal gangs and money laundering in general. The Act defined a number of serious offences regarding money laundering and racketeering. The POCA contains mechanisms for the confiscation of the proceeds of crime and for cooperation between investigators and the South African Revenue Services (SARS) Commissioner (De Koker, 2012: Com 2-7).

Money laundering was criminalised in three separate provisions in the POCA. The provisions cover the conversion, transfer, concealment or disguise of funds and the possession and acquisition of property (FATF, 2012: 6).

In the Prevention of Organized Crime Amendment Act No. 24 of 1999 the duty to report suspicious transactions was broadened to managers and employees of business undertakings. Individuals who report such transactions are allowed to raise the POCA requirements as a defence, if charged with negligent money laundering offences. In the Prevention of Organised Crime Second Amendment Act No. 39 of 1999, the focus was on defining unlawful activity but a number of smaller amendments were also made (De Koker, 2012: Com 2-10).

5.3.4. The Prevention and Combating of Corrupt Activities Act No. 12 of 2004 (PRECCA)

According to De Koker (2012: Com 2-9), the PRECCA created a number of offences relating to corrupt activities and places an obligation on a person in a position of authority to report any knowledge or suspicion that such an offence or certain offences involving an element of dishonesty, has or have been committed. The PRECCA further defines the offence of knowingly dealing or handling property that forms a part of any corrupt activities.

5.3.5. The Protection of Constitutional Democracy Against Terrorism and Related Activities (POCDATARA) Act

In South Africa the legal measures to address terrorist financing are primarily contained in the country's anti-terrorism legislation known as the Protection of Constitutional Democracy against Terrorism and Related Activities Act of 2004 (POCDATARA Act). The POCDATARA Act provides for, among other things, the criminalisation of terrorist financing activities and the freezing of assets that may be used in terrorist activities (FIC, 2012: 1-2).

With the enactment of the new terrorist legislation, the POCDATARA Act, South Africa had now complied with the combating of the terrorist financing requirements of the FATF on money laundering. The Act was legislated to criminalise the offence of terrorism and other related offences and to provide measures to prevent and combat terrorist and related activities. One of the key aims of the POCDATARA is to provide clarity on the definition of terrorism and to reduce the incidents of terrorism by criminalising, not only the offence itself, but also actions by individuals and organisations which would, directly or indirectly, aid or further terrorist activities (Scholtz & De Villiers, n.d: 258).

This legislation was researched and developed over a number of years and came into effect in May 2005. The legislation criminalises a wide range of activities including the collection of illegally-obtained funds or assets and the activities of intermediaries who may support or provide financial services to those who carry out or support terrorism. These offences apply not only to financing activities for terrorism, but also to the support of terrorist organisations and individual terrorists. During prosecution under these offences, there is no requirement for the State to

prove that a terrorist act was in fact carried out or that the funds or assets in question can be linked to a specific terrorist act (FIC, 2012: 1-2).

5.3.6. The Financial Intelligence Centre Act No. 38 of 2001 (the FIC Act or FICA)

The Financial Intelligence Centre was established in February 2002 under the FIC Act No. 38 of 2001, due to the numerous disturbing reports on suspicious and unusual transactions. The FICA set up a regulatory AML administration, to break the money laundering cycle used by organised criminal groups to benefit from illegitimate profits. The Act complements and works with the Prevention of Organized Crime Act, No. 121 of 1998 which describes the main money laundering offences. The Act's aim is to maintain the integrity of the financial system (FIC, 2001).

In 2008, amendments were made to the FICA that provide further regulatory, supervisory and enforcement of powers for the FIC and other supervisory bodies. The amendments also introduced an administrative penalty framework and registration regime for accountable and reporting institutions (De Koker, 2012: Com 2-9).

According to the FIC Act, the principal objective of the FIC is "to assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities and the financing of terrorist and related activities" (FIC, 2006).

The FICA regulator imposes certain key foundation principles namely, client identification, record keeping, reporting obligations and internal compliance structures. These requirements apply to financial and non-financial institutions and define money laundering responsibilities for the supervisory bodies (FIC, 2009/2010: 7).

Accountable institutions are required to identify their clients and verify this before any transaction may be conducted. Accountable institutions must keep records of specific information, appoint a person responsible for overseeing compliance, draft appropriate internal rules and train their employees for compliance duties.

Furthermore, every business and every employee of every business is required to report specified unusual and suspicious transactions to the FIC (IRBA, 2011: 4).

The FICA creates a framework of law and regulations to control the way accountable institutions conduct their business, particularly with reference to customer identification, record keeping, reporting, training staff and compliance requirements. The legislation places responsibility on accountable institutions for detecting potential illegal activities (Cromhout, 2002: 5).

5.4. The Financial Intelligence Centre (FIC)

Money laundering and terrorist financing are worldwide problems and require intensive solutions. As a result, South Africa formed the FIC. The FIC was established in terms of the Financial Intelligence Centre Act (2001) (the FICA) and works together with two other laws: the Prevention of Organised Crime Act (1998) and the Protection of Democracy against Terrorist and Related Activities Act (2004). The FIC is South Africa's national intelligence unit tasked to provide financial intelligence to law enforcements agencies, intelligence agencies and SARS (FIC, 2010/2011: 2, 6).

The main activities of the FIC are to enable the administration and enforcement of laws, exchange information with similar bodies in other countries, monitor and provide guidance to accountable institutions, supervisory bodies and individuals pertaining to compliance with the FIC Act; and contribute to the global AML/CFT efforts (FIC, 2009/2010: 7).

The FIC comprises of four business units: Legal and Policy, Compliance and Prevention, Monitoring and Analysis, and Administration and Support Services units. In addition, the FIC is a member of the Egmont Group and coordinates membership with the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and FATF, providing information and advice to South African representatives on an international level. South Africa and the FIC place a high priority on international cooperation to combat money laundering and terrorism financing and this is

expressed in their participation in these three international bodies (FIC, 2009/2010: 40, 48),

5.5. Monitoring Money Laundering Compliance in Financial Institutions

In a perfect world, a CRO/COO is not needed, especially if every person in a company understood the nature of risk and compliance and how to deal with risk effectively and efficiently. Unfortunately we do not operate in a perfect world and there is a need for CRO/COOs to foster compliance in companies (Steinberg, 2005: 20).

Cromhout (2002: 5) highlights that creating a culture of compliance is important and integral. A top-down approach that embraces money laundering risk management and control concepts will be the most effective and create an environment in which managers and subordinate staff are knowledgeable and aware of risks. In addition, a culture of compliance will require leadership from the top of the organisation

De Koker (2002a: 18-20) points out that although South Africa initially lacked a general money laundering control framework, the essential building blocks of a compliance system have been in place for some time. Due to a stricter exchange control system, South Africa is now a less attractive place for foreign criminals wanting to launder money.

The FICA makes provision for certain bodies, including the Financial Services Board (FSB), SARB, Registrar of Companies, various law societies, the Public Accountants' and Auditors' Board (PAAB) and the Johannesburg Stock Exchange (JSE) to supervise the compliance of accountable institutions under their control (Ford, 2003: 10-11). Financial institutions are covered by the FICA and under the Act are accountable institutions. The table below summarises the types of financial institutions operating in South Africa and the relevant supervisory bodies (FATF, 2009b: 8-10, 20).

Table 5.1 Types of Financial Institutions and their Supervisory Bodies

Type of financial institution	Authorised/registered/supervised by
Registered banks Mutual banks	Registrar of Banks, BSD (Bank Supervision Department) of SARB
Local branches of foreign banks	Registrar of Banks, BSD of SARB
Life insurance companies	FSB
Pension fund managers	FSB
Financial service providers – Category I (Brokers)	FSB – Financial Advisory and Intermediary Services (FAIS)
Financial service providers – Category II (Investment managers)	FSB – FAIS
Financial service providers – Category III (Linked investment service providers)	FSB – FAIS
Collective Investment Schemes (CIS) in securities	FSB
CIS in property	FSB
CIS in participation bonds	FSB
Foreign CIS	FSB

In addition, the FIC's Compliance and Prevention Department are responsible for the overall FICA compliance by monitoring and proving guidance to accountable and reporting institutions, supervisory bodies and other individuals regarding the performance of their obligations (FIC, 2009/2010: 49).

The JSE has described relevant obligations for exchange participants, for instance, stockbrokers are required to identify their clients, verify their particulars and maintain compliance functions. The JSE also maintains a surveillance department that monitors compliance with its rules (De Koker, 2002a: 18-20).

The sector with the most building blocks of a compliance system in place is the banking sector. Banks are required in terms of in terms of the FICA and common law to identify and verify potential clients who want to open bank accounts with the bank. Other non-banking financial institutions, for example insurance companies and foreign exchange dealers are required to have money laundering compliance programmes in place. These programmes are mainly developed by internal audit,

legal or compliance divisions who are often relied upon to support the organisations. Other initiatives include the Money Laundering Forum and the Compliance Institute of South Africa (De Koker, 2002a: 18-20).

While South Africa's legal and regulatory framework is extensive, it needs to be used more widely in future. An effective system requires that all individuals involved in money laundering or terror financing be prosecuted. A successful system should bring about a change in behaviour, reduced criminal activity and criminally-obtained funds and therefore less money laundering (FIC, 2009/2010: 8).

5.5.1. Preventative Measures for Financial Institutions

AML/CFT preventative measures have been implemented through the application of the FIC Act 2001, the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations) and the Exemptions in Terms of the Financial Intelligence Centre Act (Exemptions) (FATF, 2009b: 8-10).

The FIC Act created a range of money laundering obligations for accountable institutions. The duty to report suspicious transactions came into effect on 3 February 2003. Other obligations include customer identification, record keeping and internal controls effective from 30June 2003, through implementation of the MLTFC Regulations (FATF, 2004: 4).

Accountable institutions are prohibited from establishing a business relationship without verifying the customer's identity, and the identity of any person acting on behalf of the customer or on whose behalf the customer is acting. The MLTFC Regulations set out in detail the measures to be taken by accountable institutions when establishing and verifying their customers' identity (FATF, 2009b: 8-10).

Accountable institutions are required to keep records of information pertaining to customer identification and transactions whenever they establish a business relationship or conclude any transaction. These records must be kept for at least five years from the date on which the business relationship is terminated or when the transaction was concluded (FATF, 2009b: 8-10). Other measures include the

reporting of suspicious activities. The South African regime has a broad reporting system, which requires all financial institutions and businesses to report suspicious transactions to the FIC. The requirement is very clear on this reporting obligation and it includes attempted transactions, regardless of the amount (FATF, 2009b: 8-10).

The SARB serves as the supervisory body for banking institutions and as an overseer of South Africa's exchange control. The FSB is responsible for supervising financial advisors and intermediaries including investment managers, insurance industry, retirement funds, friendly societies, collective investment schemes, exchanges, central securities depositories and clearing houses. The JSE is a licensed exchange and self-regulatory organisation which is responsible for supervising authorised users of the exchange (FATF, 2009b: 8-10).

In order to ensure compliance with the set rules, accountable institutions are required to compile and implement internal rules to ensure that the institution and its employees take the necessary steps to comply with their AML/CFT duties, appoint an officer (Money Laundering Control Officer) who is responsible for ensuring compliance by the institution and its employees, and train its employees to enable them to comply with their AML/CFT obligations (IRBA, 2011: 19).

5.5.2. Preventative measures for Non-Financial Institutions and Professions

According to Ping (2008:323) financial and non-financial institutions need to comply with a set of obligations to prevent money laundering and terrorism financing. These obligations include measures such as a system of internal control, a customer identification mechanism, transaction and record keeping, large value and suspicious transaction reporting systems and internal training.

AML/CFT preventative measures apply to all accountable institutions, regardless of whether they are financial institutions or non-financial businesses and professions. The obligations to report activities relating to money laundering or terrorist financing, protection for reporters and the prohibition on tipping-off apply to all designated non-financial businesses and professions (DNFBPs) (FATF, 2009b: 11).

The FIC Act prescribes authorities responsible for supervising certain DNFBP sectors for AML/CFT compliance however it does not provide them with any specific powers of AML/CFT supervision or enforcement. Nonetheless, some of these authorities are using their general powers to conduct AML/CFT inspections. Though the FIC has no official supervisory functions or powers of its own, designated supervisors who wish to have FIC participation may use their general powers to appoint employees of the FIC to their inspection teams. The Centre has thus been able to participate jointly with the National Gambling Board in 25 inspections of casinos dating from October 2007 to April 2008 and 21 inspections of estate agents with the Estate Agency Board between November 2006 and June 2007 (FATF, 2009b,: 11).

5.6. The FICA View on Independent AML Compliance Reviews

According to Cromhout (2002: 5), AML risk management should be part of good governance and risk management. A comprehensive, enterprise-wide risk management strategy is one that comprises policies, procedures and controls, a compliance officer, an ongoing employee training programme and an independent testing programme.

The FICA imposes a range of compliance obligations, specifically for accountable and reporting institutions. Key compliance obligations are created by FICA regulations (De Koker, 2012: Com 6-6). The FIC and other supervisors monitor the compliance of financial institutions by verifying whether financial institutions have appropriate internal rules, training and systems to identify and report matches or close matches to listed entities. While larger financial institutions use commercial software to check accounts against the United Nations list, smaller financial institutions cannot afford such software and, as a result, there is inadequate monitoring of compliance by some financial institutions (FATF, 2009b: 55).

The FIC Act requires that accountable institutions formulate and implement internal rules to foster compliance with the Act and to make these available to each of its employees involved in transactions to which the FIC Act applies (s.42). In the implementation of internal rules, the rules must address CDD (identification and

verification), record keeping, reporting obligations and other matters that may be prescribed (FATF, 2009b: 128).

Crucial to note, the FIC Act does not specifically address the issue of an independent, internal audit function. Nonetheless there are requirements for internal auditing in some of the separate financial institution legislation (De Koker, 2012: Com 6-6).

For instance, banking institutions are subject to a general requirement to maintain an audit function (FATF, 2009b: 128). According to the Banks Act No. 94 of 1990, as amended (SARB, 1996: 57), proper bank risk management requires an independent compliance function framework to be established. The Act clearly stipulates that the compliance function should be headed by a compliance officer of the bank who shall perform his or her functions with due care and skill as reasonably expected by the MLTFC Regulations relating to banks.

De Koker (2002a: 18-20) highlights that the regulations under the Bank Act compel banks to appoint a compliance officer with senior executive status and to maintain an independent and adequately resourced compliance function. To ensure compliance, banks are also required to implement and maintain policies and procedures to safeguard against market abuse and financial fraud, including money laundering. As a minimum, these policies and procedures must be adequate to ensure compliance with relevant legislation, facilitate co-operation with law enforcement agencies, identify customers, recognise and report suspicious customers and transactions and provide adequate training and guidance to relevant staff.

In terms of the Long-term Insurance Act, long-term life insurers are required to appoint auditors who are to submit an annual audit report to the FSB. This submission should include the auditor's report on ALM/CFT compliance. Shortfalls have been noted however: this requirement does not address sample testing and much of the focus is on accounting practices, information systems, auditing and actuarial valuation processes. There are no specific references for the company board to ensure that the institution complies with all applicable laws and regulations. Likewise, general requirements apply to financial service providers to establish an

audit function but the audit functions are more focused on ensuring that the financial records of the institution are properly maintained and not on ensuring compliance with internal control rules (FATF, 2009b: 129).

In instances of collective investment schemes (under the ss. 19, 73 and 74 Collective Investment Schemes Act (CISC Act)), the Registrar is empowered to have all accounting books and financial statements audited and the results of the audit submitted to the Registrar. However, the general obligation is focused mainly on accounting practices, not compliance with relevant laws such as the FICA (FATF, 2009b: 129).

De Koker (2012: Com 6-6) argues that although aspects of these obligations may be outsourced, the institution remains liable for any compliance failure. Johnston and Carrington (2006: 55) raise the concern that outsourcing itself poses specific vulnerabilities, as functions outsourced include transaction processing and information technology, two decisive elements of AML/CFT regimes. Banks are therefore challenged with developing appropriate strategies to manage the risk inherent in outsourcing these functions, keeping in mind that the risk increases significantly when the function is outsourced to foreign entities.

De Koker (2012: Com 6-7) highlights that industry guidelines may not have authoritative bearing concerning FICA compliance, but they may have an impact on the liability for non-compliance in instances where the standard requirements are an issue.

Based on the views provided above, it seems that the FICA regulations are silent on independent reviews as an AML priority. Though there is mention of independent reviews in some frameworks, such as the Bank Act, from a national regulation and governance viewpoint it is not addressed in the FICA regulations. In certain instances where it may be presumed to be addressed however, it does not explicitly state that institutions comply with all applicable laws and regulations.

5.7. Summary

Chapter 5 provides an overview of South Africa's AML regime. The problem of money laundering is reviewed in detail and the context is provided showing how this impacts the country. In doing so, the chapter explains why money launders thrive in South Africa, what the economic conditions that attract such activities are, the role of informal business in South Africa, the general absence of formal financial and other business records and how these play a role in the abuse of such enterprises by launderers (De Koker, 2002a: 13-14).

This chapter outlines some of the key adverse effects money laundering has in the financial and non-financial sectors and some of the available preventative measures. The chapter also highlights some of the challenges such as extreme poverty, highly under-resourced government apparatus, a severe lack of skilled workers, the dominant informal sector and inadequate information and communication structures prevalent in Africa (Moshi, 2007: 9-10).

Background to the various AML laws and the MLTFC Regulations in South Africa is discussed. The Drugs and Drug Trafficking Act No. 140 of 1992, Prevention of Organised Crime Act No. 12 of 2004 (POCA), Proceeds of Crime Act No. 76 of 1996, Prevention and Combating of Corrupt Activities Act No. 12 of 2004 (PRECCA) and the Protection of Constitutional Democracy against Terrorism and Related Activities Act (POCDATARA) are evaluated in terms of AML/CFT. When and why the Acts were created and their limitations are highlighted. The chapter considers the FICA and the role the FIC plays in combating money laundering.

The FIC Act was set up as a regulatory AML administration, designed to break the money laundering cycle used by organised criminal groups to benefit from illegitimate profits. The Act complements and works with the Prevention of Organized Crime Act the POCDATATRA (2004) (FIC, 2011/2012: 6).

Lastly, the chapter refers to the research topic to address the key issue of independent AML reviews. It must be noted that although the FICA imposes a range of compliance obligations specifically for accountable and reporting institutions, the

Act does not specifically address the issue of independent AML reviews and/or the role of the internal audit function in AML compliance (De Koker, 2012: Com 6-6). FICA regulations are silent on independent reviews as an AML priority from a South African viewpoint. Although there is mention of independent reviews in some frameworks such as the Bank Act, from a FICA perspective, the rules and guidelines are ambiguous regarding independent AML reviews.

CHAPTER 6

A COMPARATIVE ANALYSIS OF SOUTH AFRICAN MEASURES AND OTHER GLOBAL GUIDELINES

6.1. Introduction

6.1.1. Background Information

The financial sector and the global economy have been victims of misconduct within the financial sector. This misconduct covers a wide range of activities linked to inadequate regulation and supervision in the sector. The financial crisis revealed that the sector was poorly organised with inadequate rules in place (Hardouin, 2011: 149-149).

Among others things, the crisis highlighted the consequences of globalisation and the interconnectivity of international markets. A key lesson that can be drawn from this is the absence of good corporate governance in financial institutions. This is attributable to a lack of customer due diligence (CDD) in business relationships (Shehu, 2010: 140).

Supply and demand are generally two sides of the same coin. There will be no supply for criminal financial services without the demand for these services and thus there will be no money laundering without money to launder (Hardouin, 2011: 151). Money laundering detection and prevention is infamously complex. Financial products, services and money laundering are dynamic and adapt over time. There are no set rules that can be applied to detect patterns of money laundering. Although fixed rules can be applied to mitigate certain extreme situations and to enforce defined regulations, these do not provide adequate safeguards against money laundering due to its adaptable nature (Gao, Xu, Wang, & Wang, 2006: 852).

As a global response to some of these challenges, the most noteworthy initiative is the FATF Recommendations advocated by the FAFT and the relevant international conventions (Goredema, 2007: xi). The FATF Recommendations have also been

endorsed as AML/CFT international standards by the executive board of the International Monetary Fund (IMF) and the World Bank and by the mutual evaluations by the FATF and associated bodies (Jensen & Png, 2011: 111).

The milestone achievement of the FATF is its comprehensive monitoring process for compliance with the AML/CFT standards. For this process, the FAFT relies on international law and concepts such as compliance, implementation and effectiveness which constitute the three critical stages in the FATF methodology in assessing countries' adherence to the FATF standards (Beekarry, 2011: 173). This rigorous scrutiny is achieved through mutual evaluation, public disclosure and the associated pressure placed on affected entities to conform (Jensen & Png, 2011: 110).

The FAFT Recommendations have been adopted by more than 180 countries. In February 2012, the FATF approved a revised set of recommendations, which now constitutes the global standard (FIC, 2011/2012: 11). Although countries are not bound to the FAFT Recommendations, they have been adopted and endorsed and commitments have been made to combat money laundering and terrorist financing by implementing the standards. The FAFT objectives are to obtain formal commitment to the standards from all governments in the FATF global AML/CFT network and to monitor compliance by conducting evaluations, performing follow-up checks after evaluations and identifying high-risk or uncooperative jurisdictions (Shehu, 2010: 141-142).

In order to protect the international financial system from money laundering and terrorist financing risks and to encourage better compliance, the FATF identified jurisdictions that have strategic deficiencies and works closely with them to address those these problems, particularly those that pose a risk to the international financial system (FAFT, 2011).

The assessment of the effectiveness of a country's AML/CFT system is as important as the assessment of technical compliance with the FATF standards. These two aspects are also not exclusive of each other. A country's level of technical

compliance contributes to the positive assessment of its effectiveness (FAFT, 2013: 14-16).

The fight against money laundering in low-income countries faces a number of challenges regarding the implementation of FAFT standards. The concerns raised are

- government resources are scarce and there may be other areas needing urgent attention besides the financial sector
- a severe lack of resources and skilled works to implement the programmes
- legal institutions have weaknesses
- the informal sector dominates and economies are cash-based
- poor documentation and data retention systems and
- a very small financial sector with limited exposure to global international systems in some instances (Shehu, 2010: 149).

Approximately 118 countries have been assessed for their level of compliance with international AML/CFT standards since 2004. The assessments include 24 developing member-countries of the Asian Development Bank (Jensen & Png, 2011: 110). The number of countries assessed using the 2004 methodology has grown to 145 between 2004 and 2009 and 123 reports have been published on these assessments (Beekarry, 2011: 174).

The FATF has 36 members including South Africa, which is the only African representative (FIC, 2011/2012: 11). South Africa officially joined the FATF in June 2003 (De Koker, 2012: 1-13). Although South Africa became a member in 2003, initiatives to address money laundering in the country date back to the 1990s while measures to combat the funding of terrorism are more recent (Goredema, 2007: 73).

6.1.2. Challenges in the South African Informal Financial Sector and Economy

The misuse of the informal sector by money launderers is a general cause for concern because the current money laundering laws and regulations mainly cover the formal sector. The informal business sector in South Africa is large and the lack of financial and other business records make it easier for money launderers to abuse the system. Informal business serves as a suitable vehicle because it is difficult to dispute a business's alleged turnover in relation to its actual turnover without records (De Koker, 2002a: 13-14).

Large amounts of cash flows in community-based credit schemes that operate general communal savings arrangements (e.g. stokvels) or dedicated savings schemes (e.g. burial societies). There are also a number of organisations that operate on the outer reaches of the regulatory systems and these include NGOs, charitable institutions and religious organisations. Through these schemes, illegally-obtained funds can be layered and integrated into the informal sector without entering the formal sector of the economy (De Koker, 2002a: 13-14).

Underground banking systems, in the form of hawala systems, are also operating in South Africa within specific ethnic communities (De Koker, 2002a: 13-14). The word 'hawala' has an Arabic origin and the word used to mean 'change'. In Hindi and Urdu it means 'trust' which is the underlying principle of the hawala system (Shanmugan, 2004: 37). These systems provide a high level of anonymity and can easily be abused by money launders to circumvent scrutiny by law enforcement agents (Moshi, 2007: 2). Hawala systems have been used for many years to avoid exchange control restrictions and expensive foreign exchange transaction fees (De Koker, 2002a: 13-14).

Hawala is an alternative remittance system and exists and operates outside of or parallel to the traditional banking system. It was first developed in India, prior to the introduction of Western banking systems, and is currently a major remittance system used around the world. Two basic principles distinguish the system from others: trust and the extensive use of connections including family relationships and regional

affiliations. Money transfers are based on communications between members of a network of hawala dealers (Financial Crimes Enforcement Network, n.d.).

Operating parallel to the financial systems, hawalas offer anonymity for international transfers and also include securities, insurance and money-changing enterprises (Mulig & Murphy, 2004: 24). Particularly in countries with limited financial capacity IFT systems, such as hawala, play a critical role. The growth of hawalas is mainly due to its ability to facilitate trade between distant regions, especially when traditional banking instruments are either weak or absent, lower transactions costs, speed of transactions, cultural convenience and potential anonymity (Qorchi, Maimbo, & Wilson, 2003).

The increase in South African property prices made the real estate sector an excellent investment for anyone with sufficient funds at their disposal regardless of whether these funds were derived from criminal or legitimate activities. An important factor behind the popularity was that South Africa had a very sophisticated banking infrastructure making it relatively easy to move funds around regardless of exchange controls (Goredema, 2006: 7).

Within the financial sector, automatic teller machines are also used on a large scale to deposit and withdraw money. Automatic teller machines that offer the service of generating bank cheques have featured in numerous laundering schemes. Bearer documents such as negotiable certificates of deposit have been employed in more sophisticated schemes (De Koker, 2002a: 3-14).

Several cases involve insurance products that were used to launder money. A typical example is where single premium policies are paid in monthly premiums with illicit proceeds. The launderer would make an overpayment and then request a repayment of the excess amount. When the insurance company repays the excess amount the launderer associates the transaction with an insurance pay-out. Some of the most common cases involve the launderer buying and surrendering policies (De Koker, 2002a: 3-14).

These unlawful practices distort business decisions, increases the risk of bank failure, violate economic policy, harm the country's reputation and expose its people to drug trafficking, smuggling and other criminal activity (FIC, 2006/2007: 10). Despite the views raised, Johnson and Carrington (2006: 53) argue that it is unreasonable to expect that financial institutions will not be used as vehicles for money laundering or terrorist financing however, AML/CFT systems should be adequately designed and applied to address these inherent risks. In instances where failures have been identified, regulators will review the bank or financial institution's system to obtain assurance that appropriate policy, practices and internal controls are in place and used in future.

6.2. FAFT Recommendation Compliance in South Africa

South Africa joined the FATF in June 2003 (De Koker, 2012: 1-13). Development of systems to implement the FATF standards is an ongoing process. Monitoring the level of compliance with FATF standards is an effective way to ensure that the actions taken by national authorities are consistent and improved as necessary (Shehu, 2010: 147).

Shehu (2010: 147) argues that over time the mutual evaluation conducted by the FATF and other relevant organisations has proven to be a useful tool to ensure compliance to the standards. However, Moshi (2007: 9) states that from an African viewpoint a 'one-size-fits-all' approach is bound to fail because Africa is different to other continents.

In 2003, South Africa's money laundering control received a generally positive evaluation from the FATF. The report highlighted significant compliance with the 1996 FATF Recommendations and pointed out areas for improvement (De Koker, 2012: 2-13). AML/CFT systems are still a work in progress but South Africa has shown a firm commitment to implementing them and there is a close cooperation and coordination between a variety of government departments and agencies (FATF, 2009b: 6).

Since 2003, South Africa has taken numerous steps to address many of the recommendations that were made in its first FATF mutual evaluation report (FATF, 2009b: 6). In 2008, South Africa underwent a much closer evaluation by the FAFT and the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) based on the FATF 2003 revised 40 + 9 Recommendations (De Koker, 2012: 13). The results of the review showed that South Africa was compliant with 8 of the 49 Recommendations and was rated as "largely compliant/partially compliant" for the majority of the Recommendations but indicated that more work needs to be done to move towards meeting the FATF standards (De Koker, 2012: 2-13).

In 2008 another evaluation was performed by the FATF. The evaluation of the AML/CFT programme was based on the 40 Recommendations and the Nine Special Recommendations on Terrorist Financing. The evaluation was based on the laws, regulations and other materials supplied by South Africa during the FATF's visit to South Africa in August 2008 (FATF, 2009b: 5).

South Africa has passed various laws aimed at combating money laundering. The main criminal legislation is the FICA which created the administrative framework for money laundering control (De Koker, 2002a: 3).

Regarding compliance with the FAFT standards, South Africa was found to have a number of deficiencies requiring improvement. The FATF report highlighted several weaknesses in the FICA regulations (FATF, 2009b: 131).

With regard to the FATF Recommendation No. 5 pertaining to CDD and record keeping, the FAFT highlighted a number of gaps in the systems and regulations. Despite the efforts to verify customer's identity, the FATF (2009b: 8-10) found that there was no specific requirement in the FICA requiring accountable institutions to identify or verify the identity of beneficial owners (i.e. the natural persons who ultimately own and control the customer). Additionally, a limited number of financial institutions were not subject to AML/CFT supervision because they are not defined as accountable institutions in terms of the Act. There was also no designated supervisory authority for institutions such as the Post Bank and members of the Bond Exchange.

The FATF (2009b: 8-10, 108) also pointed out that, with the exception of the banking sector, there is generally no obligation to keep transaction records sufficient to allow a reconstruction of account activity. There was no requirement to maintain account files or business correspondence as part of the record keeping obligation and uncovered financial institutions were not subject to the record keeping obligations in the FIC Act. The record keeping requirement was somewhat eroded by some of the FICA Exemptions which excused accountable institutions from maintaining records of customer identification and verification. Certain Exemptions fully discharge some accountable institutions from all CDD requirements (as well as some or all record keeping requirements) particularly in circumstances defined as low-risk. This is contrary to the FATF Recommendations which allow for simplified but not full exemption from CDD requirements.

With regards to Recommendation No. 13 on the reporting of suspicious transactions, South Africa was assessed as poorly compliant due to the fact that leasing and financing companies had not yet implemented the reporting obligations (FATF, 2009b: 127).

In line with Recommendation 15, FAFT requires, among other things, that financial institutions should develop internal policies, procedures and controls supported by appropriate compliance management, as well as an audit function to test these systems (FATF, 2003: i). The key findings raised by FATF, with particular reference to recommendation 15 and the FICA requirements, included the fact that there are no requirements for 1) accountable institutions to maintain an adequately resourced and independent audit function to test the compliance systems in line with the AML/CFT procedures, policies and controls; there is no general requirement for financial institutions to put in place screening procedures to ensure high standards when hiring all employees; there is no requirement for training to be conducted on an ongoing basis; and, moreover, uncovered financial institutions are not subject to the FICA requirements relating to internal controls. (FATF, 2009: 131)

6.3. Comparative Analysis of Independent Anti-money Laundering Reviews

According to the FATF (2012: 78), financial institution programmes against money laundering and terrorist financing should at least include the development of internal policies, procedures and controls and independent audits function to test the system. FATF guidelines are clear on the requirements of an independent auditing function to test the system.

The FATF (2009b: 128-129) asserts that an auditing function performing AML compliance reviews must be functionally independent, objective and sufficiently resourced so as to provide an independent assessment on the adequacy of and compliance with the bank's established policies, processes and procedures. To ensure independence, the compliance officer should have direct access to and support from the CEO of the bank, and should report non-compliance with laws and regulations or supervisory requirements to the bank's CEO, board of directors and audit committee (Banks Act Regulation 49(4)(b) and (d)).

The FAFT Recommendations are clear about the need for an independent audit function to test systems but who should perform the independent testing of systems was not explicit. The research seeks to identify who is in the best position to test and provide assurance of AML systems.

The position in the UK and the EU is rather interesting. The EU AML Directives and JMLSG guidance contain no recommendations on independent AML reviews (Delston, 2007: 6). The money laundering rules made by the FSA impose five main duties which include "know your customer" (KYC), keeping records, establish an MLRO to ensure that money laundering suspicions are reported internally and externally and having a system of internal controls in place to prevent money laundering (Leong, 2007: 144).

The UK rules highlight that it is the MLRO, not the independent party, who has to report at least annually on the operation and effectiveness of AML system and controls while the EU Directives are silent on the issue of independent AML reviews.

The FSA rules place responsibility on the institution itself to carry out regular assessments of the systems and controls to ensure compliance with set rules but the JMLSG guidance contains no recommendations on independent reviews. It is thus fair to assume that the EU and UK's AML regimes do not endorse independent AML reviews (Delston, 2007: 6).

The position of the US is clear on independent AML reviews. The US Patriot Act of 2001 (US Government, 2001: 322) states that a "financial institution should establish anti-money laundering programs … including the designation of a compliance officer … and an independent audit functions to test programs".

The US Patriot Act supports independent auditing of AML systems. The legislation in the Patriot Act represents an opportunity for institutions to continually review their compliance programmes and make necessary improvements. This component creates a safety net and provides some level of confidence that AML programmes are working as intended by ensuring that there is an ongoing self-monitoring programme to either validate the processes or identify and correct errors in procedures as soon as possible (Risk Solutions Financial Services, 2007: 8-9). Furthermore banks should rely on continuous monitoring and independent analysis to ensure that problems are detected (Maranto, 2006: 56).

The US Department of the Treasury (2006: 2-3) stresses that the primarily the purpose of an AML independent review is to monitor the adequacy of the business' AML programme. The review is mainly intended to determine compliance with the requirements of the Bank Secrecy Act (BSA) and the business' policies and procedures.

Shonk (2007a: 9) emphasises that AML programmes must provide an independent review of compliance with the BSA and ensure that a thorough compliance audit is performed frequently, that it is adequately documented and conducted with appropriate segregation of duties.

The BSA requires financial services businesses to establish AML programmes that include an independent audit function to test programmes. The Act requires written policies and procedures that provide for independent reviews to monitor and maintain an adequate programme (US Department of the Treasury, 2006: 1).

From a South African viewpoint it is clear that FICA regulations do not explicitly endorse independent reviews as an AML priority. There is some mention of independent reviews in some financial institution frameworks but it is not adequately addressed for AML purposes in terms of national FICA regulation and governance.

A key feature not highlighted in the FICA is that it does not explicitly address the issue of an independent, internal audit function or independent AML reviews as a priority. Nonetheless there are requirements for internal auditing in some of the separate financial institutions legislation (De Koker, 2012: Com 6-6).

The table below provides an overall summary of the various AML guidelines that have been reviewed and their stance on independent AML reviews.

Table 6.1 AML Guidelines and Independent Reviews

AML Regimes Reviewed	Key Guidelines/Legislature	Independent AML reviews contained in frameworks/legislature
Financial Action Task Force	FAFT Recommendations	Yes
United Kingdom	JMLSG Guidance Notes	No
European Union	AML Directives	No
United States of America	US Patriot Act	Yes
South Africa	Financial Intelligent Centre Act	No

6.4. Summary

This chapter looks at South Africa's AML compliance with particular reference to the FATF standards. The review conducted on South Africa in 2003 was generally positive but also highlighted several areas for improvement (De Koker, 2012: 13). In

2008 another evaluation was performed by the FATF based on the 40 + 9 Recommendations (FATF, 2009b: 5). Though there was improvement made the 2008 report emphasised several weakness with the FICA regulations (FATF, 2009b: 131).

This chapter provides an overview of the AML regime in South Africa. It looks at three critical areas: where the country began in terms of AML/CFT, where the country currently stands in this regard and what needs to be done to move forward towards becoming a fully compliant member of the FAFT.

The second half of this chapter reviews the various AML regimes and their views on independent assessments and considers the US Patriot Act, the EU AML Directives, the UK guidelines, the FIC Act and other supporting AML regulations in South African.

In summary, the FATF guidelines are clear on the importance of an independent audit function to test AML systems (FATF, 2012: 78). The US is unambiguous regarding independent AML reviews as a priority (US Government, 2001: 322). Independent audits do not feature explicitly in the EU Third Directive (Delston, 2007: 6) while the FIC Act does not specifically address the issue of independent AML reviews as a priority (De Koker, 2012: Com 6-6).

CHAPTER 7

INTERNAL AUDITING AND ITS ROLE IN PERFORMING INDEPENDENT AML REVIEWS

7.1. Introduction

7.1.1. General Background

One does not need to occupy the CEOs chair to recognise the rapid changes occurring in the business arena. News publications regularly report on corporate scandals and frauds and the resulting laws and regulations seem to suggest that the situation will become more complicated. Leaders in the business community forecast further changes and increased organisational risks which will lead to compliance implications (IIA, 2013b).

Money laundering and terrorist financing today pose an immense challenge to the stability, integrity and reputation of the financial sector and society as a whole. The process of globalisation and the increasing mobility of capital have intensified these threats. Organised crime takes advantage of globalisation to launder money (Ganguli, 2010: 1). Thus we continue to see foreign governments strengthening their AML programmes and multinational bodies issuing additional guidance (Beaumier & Shah, 2003: 14).

Financial criminals continuously find new ways to launder money. Money laundering techniques have become more sophisticated over the years. To meet the increasing regulatory expectations and minimise money laundering risk it is important to be informed of how money launders perpetuate their crimes (Shonk, 2007b: 56). Internal auditors can help detect and deter money laundering and terrorist financing activities by assessing fraud and money laundering risks (Sinason et al., 2003: 11).

Although the basic goal of money laundering is no different today than decades ago, money laundering is now taking place in a high-tech, global environment. The most

serious aspects of money laundering are not necessarily the crime itself, the major concern is that it provides criminals with access to the proceeds of their criminal activities. These proceeds can be used in several of ways to commit other crimes including drug trafficking, organised crime, terrorism and others (Mulig & Murphy, 2004: 22).

7.1.2. Money Laundering and Internal Auditing

Large sums of money are laundered through financial institutions, appearing at one institution and then disappearing just as quickly, and this undermines the integrity of financial institutions. Since 9/11 and other global events, concerns have been raised and there have been increased responsibilities for accountants and internal auditors regarding money laundering. As many interested parties realise the need for global efforts to combat money laundering, internal auditing has provided a unique opportunity and an obligation has arisen to take a proactive role in these efforts (Mulig & Murphy, 2004: 22-25).

Very few documents have had such a profound impact on the profession as the King III Report that came into effect from 1 March 2010. The King III Report focuses on the internal audit profession in South Africa. It advocates and champions the importance and the value of internal auditors as a key part of governance in organisations. It has propelled the profession into centre stage and continues to put the spotlight on the need to ensure that internal auditors are able to meet the increased expectations of the profession (IIA, 2012b: 8).

Given the pervasive nature of money laundering techniques, forensic accountants and internal auditors are required to develop an understanding of the nature of money laundering. It is important to understand the areas of risk, internal controls and red flag indicators (Sinason et al., 2003: 18). These phenomena point to new demands, challenges and opportunities for management, the board and to the need for competent internal auditors. Today, more than ever, internal auditing is crucial to corporate governance, risk management, effective internal control and efficient operations (IIA, 2013b).

To cope with the challenges, internal audit must evaluate its capabilities and, where necessary, obtain appropriate resources. Adequate planning is fundamental to ensuring that the required personnel and tools are available when needed (Agarwala, Girling, & Makol, 2008: 28).

Internal auditors, particularly in banking and other financial services, have to respond to new challenges, changes and expectations in today's working arena. Although companies in the financial sector tend to have sophisticated internal audit departments, expectations for improvements continue to grow (Rossiter, 2007: 34).

The business environment has changed amidst the recent economic decline experienced by many organisations. New risks that influence business success have come to the fore and these illustrate the importance of identifying and assessing strategic risks. Strategic plans that focus on introducing new products, entering new markets, adapting the sales model, outsourcing functions or making other substantial changes expose organisations to new challenges and vulnerabilities. Internal auditing can play a key role in identifying and monitoring strategic risk across the organisation (Martin, 2013: 25).

Evolutions in the global corporate environment have also raised the profile of the role played by internal auditing. The ever increasing demands placed on internal auditors lead to changes in the requirements of both management and the audit committee (Betts, 2008: 74). Through their unique positioning internal auditors can be considered as a line of defense for the board. Internal auditors have the right to access all information in the organisation and therefore all stakeholders will be direct beneficiaries of an effective internal audit function which will inevitably provide value to other cornerstones of corporate governance (De Smet & Mention, 2011: 186).

At a strategic level, the internal auditing function helps the organisation's board and senior management to identify and mitigate exposures associated with pursuing strategic objectives while the related entity and process level exposures receive attention as well. The internal audit function serves as a management tool for senior

management and the board and the value of auditing extends far beyond compliance and assurance services traditionally associated with the field (Martin, 2013: 25).

Such diversity gives internal auditors a broad perspective of the organisation and makes them an invaluable resource to executive management and the board of directors for achieving the overall goals and objectives of the business, as well as reinforcing internal controls and organisational governance (IIA, 2013a).

7.2. Background to Internal Auditing

7.2.1. What is Internal Auditing?

According to the Institute of Internal Auditors (IIA), internal auditing is

> an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (IIA, 2013a).

This definition of internal auditing is accurate and can be considered a guide to setting department objectives. Effective internal auditors serve the organisation's corporate consciousness by advocating operational effectiveness and efficiency, managing internal controls and risks, supporting the organisation to meet its objectives and goals and by advising and making recommendations to management, the board of directors and the audit committee (Joubert, 2008: 14).

Internal auditing should be performed by professionals with an in-depth understanding of the business culture, systems and processes. The activity provides assurance that internal controls in place are adequate to mitigate the risks, that governance processes are effective and efficient that and organisational goals and objectives are met. In performing reviews, emerging technologies and new opportunities are considered, global issues are examined and risks, controls, ethics,

quality, economy and efficiency are assessed. Providing assurance that the controls in place are adequate to mitigate the risks is a core auditing function (IIA, 2013a).

Internal auditing is a profession that has been redefined over the years. Despite confusion and dysfunction that has occurred during its evolution, internal auditing has changed rapidly. Currently, internal auditors are a support for management. Initially focusing on financial and accounting matters, internal auditing has always redefined itself over the years to meet the changing needs of entities by updating its objectives to detect principal risks and assess internal controls (Iovitu et al., 2013: 299-300).

In a research conducted by PricewaterhouseCoopers (PwC), a question was raised as to how reassurance is given that risks are being managed, with particular focus on the role of the internal auditor. The role of internal auditing continues to be an area of debate. At one extreme, organisations allocate wide-ranging authority to internal auditors regarding compliance while another alternative argues that the focus should be on major risk assurance and control (Betts, 2008: 74).

Many organisations worldwide are under pressure to responsibly asses and manage enterprise risks. Changing compliance and governance challenges are forcing organisations to ensure that their internal auditing functions are operating effectively and efficiently. Internal auditors must ensure that risk management, internal controls and governance processes accomplish business objectives and meet stakeholder expectations. If there is going to be any value in the improvement and effectiveness of an internal audit function, there has to be a comprehensive understanding of the specific objectives, risks and priorities relevant to an organisation (Machaba, 2012: 15).

On the other hand internal auditing is primarily driven by management's desire to have an internal resource that attends to organisational processes and ensures accuracy, efficiency and effectiveness of operations (IIA, 2005: 32).
Nonetheless Von Eck (2011: 6) draws attention to the view that there is a general lack of understanding over what internal auditing is and the role of the profession.

Many organisations establish internal auditing functions purely from a compliance perspective without understanding the value it can add. Organisations should understand the role of internal auditing as a key assurance provider for the board of directors through the audit committee.

7.2.2. International Standards for the Professional Practice of Internal Auditing (Standards)

Internal auditing is performed in different legal and cultural contexts within organisations that vary in purpose, size, complexity and structure. While many differences may affect the practice of internal auditing in each environment, compliance with the IIA International Standards for the Professional Practice of Internal Auditing (Standards) is a fundamental principle in meeting the responsibilities of internal auditing. The composition of the standards is divided between Attribute and Performance Standards. Attribute Standards address the attributes of organisations and individuals performing internal auditing while the Performance Standards describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured (IIA, 2012c: 1).

The purposes of the Standards are to:

- delineate basic principles that represent the practice of internal auditing,
- provide a framework for performing and promoting a broad range of value-added internal auditing services,
- establish the basis for the evaluation of internal auditing performance and
- foster improved organisational processes and operations (IIA, 2012c: 1).

7.2.3. Reporting to an Audit Committee

The IIA Standards require the chief audit executive (CAE) to report to a higher level within the organisation as part of their responsibilities. It is the view of the institute that, to achieve the necessary independence, the CAE should report to the audit committee or its equivalent, whereas, for administrative purposes, the CAE should report to the CEO of the organisation (IIA, 2004: 38).

A functional reporting relationship establishes a link between positions or organisational units at different managerial levels based on the unique nature of the function for which a mutual responsibility is shared. At times this may seem ambiguous since a functional reporting line is much stronger than an administrative one because the functional body controls an individual's compensation and evaluations (Tabuen, 2013: 28).

As a result, internal auditing is ideally positioned to assist the audit committee by providing oversight and assurance for the entire organisation. Risk management processes form part of this and involve the design and its operational effectiveness, the effectiveness of the controls and responses to them, verification of the reliability and appropriateness of the risk assessment and reporting the risk and control status to various stakeholders (Dinga, 2012: 16).

7.3. Types of Reviews Performed by Internal Auditors

According to the IIA (2013a), internal auditing is "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations". This is indicative of another aspect of internal auditing: the provision of consulting services that improve business operations. Given the nature of money laundering and from a risk perspective, internal auditors are well positioned to provide assistance to a business from a consultancy viewpoint. Consulting services are advisory in nature and are usually performed at the request of a client. The nature and scope of the consulting arrangement are subject to an agreement with the client (IIA, 2012c: 2).

Middle management faces assurance and compliance requirements and will seek consultation and direction for operational improvements. Rather than determine the level of risk associated with various processes and then provide an appropriate level of monitoring, the internal audit function can enable operational managers to implement practices that substantially reduce risk exposure and enhance efficiency. By becoming partners in identifying exposures and enhancing compliance measures

throughout the organisation internal auditing becomes a catalyst for continuous improvement (Martin, 2013: 26).

From an auditing viewpoint, Burnaby and Hass (2004: 15) highlight that there are mainly four types of strategies. These are the internal controls and compliance reviews, control self-assessments, outsourcing and process improvements and business leadership development. Compliance reviews are an auditing strategy that requires a high level of auditor experience. The objective of the auditing staff, as determined by senior management and the board of directors, is to ensure compliance with regulatory requirements.

There are different tiers of auditing according to certain theories. The first tier is purely compliance related and considers the compliance function mandate, framework and documented processes. The second tier looks at specific legislation and expresses an opinion as to whether the compliance monitoring and subsequent reporting is adequate. The third tier addresses operational compliance to ensure that the compliance function works closely with the other business functions (Terblanché et al., 2008). When performing these types of audits, the auditor frequently identifies unusual and suspicious activity and any such findings should be reported to management immediately (Sartip, 2008: 58).

7.4. Compliance and its Relationship to Internal Auditing

The size of an institution and the industry within which it operates influence the need for a compliance function as well as an internal auditing function. Different industries will have different needs regarding compliance and internal auditing (Terblanché et al., 2008). Compliance risk may even be more important for auditors to focus on than financial risk. Companies are now considering how to streamline compliance testing in order to cope with redundant and overlapping requirements (Whitehouse, 2013b: 10).

Compliance assessment is primarily a mechanism through which the function can assess the quality and effectiveness of the AML programme in place. The auditor's responsibility is to ensure that these components operate effectively, that periodic

assessment are performed by sufficient and qualified professional staff and whether the results of these reviews are being reported and acted upon by management (Sartip, 2008: 58).

Sharon (2006: 12) argues that there seems to be a confusion regarding the role of the compliance function and the role of risk management. In many organisations risk management is part of the auditing function but the question has arisen as to whether auditing has become part of risk management. Consistent with the view of Sharon, Von Eck (2011: 6) argues that a number of Internal auditing departments are established purely for compliance without understanding of the value internal auditing can provide from an assurance perspective.

International best practice prescribes that compliance monitoring be performed by the compliance function and not by internal auditors. One of the key reasons is that the compliance department is in a better position to monitor operations on a continual basis whereas internal auditors may only be able to monitor compliance on an annual or bi-annual basis. It is therefore crucial that a compliance function operates effectively and is properly coordinated by means of an internal audit function. In some instances there are legislative or industry requirements that prescribe that the internal auditing be a separate function from compliance (Terblanché et al., 2008).

Current trends show that many industries are becoming highly regulated. For example, banks, insurers and retailers have certain requirements and legislation to comply with. In the banking and insurance industry the monitoring of adherence to specific legislative requirements is performed by the compliance team. In organisations where compliance is still in its infancy stages, monitoring is often assigned to internal auditors (Terblanché et al., 2008).

The recommended practical relationship between internal auditing and compliance involves various aspects and tasks. Internal auditors should perform periodic audits on the compliance function to assess the level of adherence to the set compliance framework and in order to provide feedback in an audit report regarding non-

compliance with specific legislation. Action plans and target dates to correct deficiencies should also be identified by auditors to ensure that the results of these audits are communicated to management, the risk committee and the audit committee. Significant issues of non-compliance should be escalated to the appropriate board committee. Solutions and plans to rectify identified problems should be reported to the risk committee as part of the enterprise risk management (ERM) framework and action taken to resolve the problems (Terblanché et al., 2008). Internal auditors play an important role in the monitoring of ERM but do not have the primary responsibility for its implementation and maintenance (Sharon, 2006: 12).

Internal auditing is at the centre of corporate governance systems and performs a crucial function by improving the organisation's system of controls. By conducting reviews of critical controls at every level of the organisation, internal auditors can provide assurance that key controls are properly designed and operate effectively (De Smet & Mention, 2011: 182). However, internal auditors should not perform compliance monitoring and ideally should only be positioned to provide assurance on the compliance process for a specified period. Ideally audits of the compliance function should be carried out annually to provide an opinion on whether or not the compliance requirements are being met (Terblanché et al., 2008).

7.5. Anti-money Laundering Compliance from an Internal Auditing Perspective

7.5.1. Compliance Risk Assessment

As regulatory pressures increase and institutions come under scrutiny the internal audit function must identify key risks and challenges earlier on and more efficiently than in the past (Agarwala et al., 2008: 25).

Assessing these risks is an essential part of an organisation's ERM process. Examining compliance-related exposure and vulnerability must be part of the risk assessment process. Internal auditors are in a position to assess possible areas for vulnerability to corruption at all levels and report their findings, along with their assessment of the accompanying controls, to senior management. This also enables

auditors to consider corruption risks during a risk assessment, specifically checking whether the organisation is in compliance with federal and international laws (IIA, 2012d: 29). It is important to understand that money laundering is a serious risk and, particularly, a compliance risk.

7.5.2. Similarities between a Risk-Based Approach to Money Laundering and Risk-Based Auditing

It is worth noting that risk has always been an integral part of AML policies, even for a rule-based approach. However, the concepts risk, risk assessment and risk management have now become central themes in the preventative AML/CFT policies (Ross & Hannan, 2007: 107).

Maranto (2006: 56) argues that a risk-based analysis across all business lines and products can help banks identify and implement proper procedures to address potential weaknesses. When a bank has a documented risk-based methodology regarding due diligence, transaction monitoring and AML compliance efforts, it should be able to support its decisions.

Countries are required to identify, assess and understand the money laundering and terrorist financing risks and should take appropriate action. Resources should be applied to ensure that the risks are mitigated effectively. Based on the risk assessments, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach involves efficient allocation of resources for the AML/CFT regime and the implementation of risk-based measures in line with the FATF Recommendations (FATF, 2012: 11).

It is not possible to audit all processes within a year because of resource limitations but resources should be allocated to areas where the organisation can derive the most benefit. The internal auditors should plan their auditing processes to fit into a three-year period or in accordance with the audit committee's needs. The audit priority risk model is used to determine the risk of a process from an internal auditing

point of view and generally high-risk areas are audited rather than low risk areas (Joubert, 2008: 21-22).

Based on the views expressed above, there are clear parallels between the risk-based AML method and the risk-based approach followed by internal auditors when reviewing an organisation. The risk-based approach, championed by the FATF recommendations, states that more resources should be channelled towards areas of high risk first then to medium and low risks. It may thus be assumed that process and control audits should mainly be based on high risk areas. Much benefit can be derived from this method because it means that areas receiving the greatest attention from a money laundering perspective will also receive similar attention based on the risk based methodology applied by internal auditing.

7.5.3. Are there Effective Standards, Policies and Processes to Address Compliance Risk?

The IIA Standards set the bar for effective internal controls. Policies, procedures and processes should be designed in such a way that they support and contribute to the effectiveness of the Standards and uphold the prescribed code of conduct. Internal auditors are well positioned to determine whether policies and procedures are being followed, to assess the risk management practices in order to mitigate compliance exposures and evaluate the effectiveness of the organisation's internal controls to manage and mitigate compliance risk (IIA, 2012d: 29).

7.5.4. How is Inappropriate Conduct Detected and Monitored?

In any dynamic environment, it is critical that internal control keeps pace with change. An important role for internal auditors is to assess and provide an opinion regarding the adequacy of internal controls to mitigate the organisation's compliance risks. This is done firstly by checking the design of the controls and then determining whether they are operating effectively. There may be instances where existing controls are inadequate and the internal auditor's role may then be to offer recommendations to management regarding the design and/or operational improvements that can be made (IIA, 2012d: 29).

Organisations are required to take reasonable and steps to evaluate and provide a form of assurance regarding the efficacy of compliance and ethics programmes. Processes such as control self-assessment (CSA) are often implemented to review compliance programme effectiveness. Other methods include tracking activities to determine whether recommendations by the internal auditors' have been implemented, providing statistics on employee complaints and disciplinary actions and gauging the level of training that has been provided. Having performed all these initiatives, information must be gathered and an in-depth assessment should take place to determine whether enough is being done to ensure the necessary compliance (IIA, 2012d: 30).

In this way, internal auditors are well positioned and equipped to be key role players. Often internal auditors find themselves directly involved in some aspects of risk management assessment, conducting CSA workshops, collecting data on for implementing recommendations and assessing whether there are gaps in employee training (IIA, 2012d: 30)

7.6. Why Internal Auditing is Well Positioned to Provide Independent AML Assurance

7.6.1. Internal Auditing Independence

Auditing and compliance professionals are not all equally independent. True independence was viewed ideally as someone from outside the company classically defined as a gatekeeper. The gatekeeper is viewed as an outsider with a career and assets beyond the firm and thus has less to lose than the inside manager. A different view has been raised regarding the gatekeeper function. All internal employees have a vested interest in the company's success and cannot be viewed as independent but some commentators have noted that certain internal functions may be better suited to the role of gatekeeper (Tabuen, 2013: 28).

An independent function offers objective assurance and consulting activity designed to add value and improve organisation an organisation's operation. By establishing

its value as a resource for objective and independent oversight and counsel, the internal auditor's function gains stature and credibility among organisational leaders, as well as line managers (Martin, 2013: 26).

The internal audit function is designed to accomplish this through a systematic, disciplined approach. The approach requires an evaluation of and improvements to risk management, controls and governance processes. As a result internal auditors have a vantage point that provides independent and objective insight into the organisation (Martin, 2013: 26).

The degree of integration between a business, the compliance function and internal auditing is often a key to a successful and effective AML programme. Although internal auditors should operate independently from both compliance and other business functions they are still required to provide unbiased recommendations for improvement, and therefore a culture of cooperation and collaboration is critical among these departments for an AML/CFT programme to succeed (Axelrod & Ross, 2012: 73).

Tabuena (2013: 28) observes that the majority of the CAEs report to an audit committee and there is an agreement that such reporting enhances internal audit independence. Inside the organisation, internal auditing and compliance have served as gatekeepers. Their formal and informal communication channels mean they are well positioned to access critical information that may expose any company misconduct. Internal auditing and compliance therefore more independent than legal and finance functions and therefore better suited to the gatekeeper function.

7.6.2. Understanding Controls and Processes

At the centre of AML is a system of internal controls. The first step in implementing an AML compliance system is to establish a set of internal controls. Controls will differ between institutions and the level of their sophistication will also differ depending on the size, structure and risk profile of a financial institution (Husisian, 2010: 17).

An effective AML/CFT compliance programme is one that establishes internal controls that are developed in response to an organisation's risk assessment and that manage those risks according to the risk tolerance of the institution. Therefore it is pivotal for an institution to evaluate its unique risks by considering factors such as customers, geographical locations and products and services offered to customers (Risk Solutions Financial Services, 2007: 4)

Banks and other financial institutions must be sufficiently knowledgeable of the components of a good AML programme to effectively perform due diligence. They also need to work on data transmission issues and ensure adequate internal controls are in place (Costanzo, 2008).

Accountants and internal auditors are more liable and responsible for ensuring that companies have adequate systems of internal control in place and such procedures should detect and prevent money laundering schemes (Mulig & Murphy, 2004: 22).

An internal auditing function exists in many organisations, regardless of size and objectives. The methodology is universal to all activities and allows for better control. Internal auditors can evaluate internal control systems and give reasonable assurance regarding the general management functionality (Iovitu et al., 2013: 300).

An internal audit measures and evaluates business control systems and can be relied upon by management. This is accomplished by continuously reviewing the effectiveness of internal controls and the efficiency of operations regarding other compliance requirements stemming from policies, laws and regulations (Veazie, 2011: 9). Internal auditing provides opportunities for improving management control and helps the organisation accomplish its objectives by recommending improved operational and control method, and enhanced risk management (Joubert, 2008: 15).

Furthermore, as an internal control specialist with an auditing acumen, internal auditors have a sound understanding of the accounting, internal control and auditing issues that should be addressed in the design of effective audit committee policies and procedures (Ligthtle & Bushong, 2000: 39). Competent internal audit

professionals bring objectivity, integrity and communication expertise to a review. Auditors are also able to identify risks in all areas of a business and have the skills to assess the effectiveness of controls put in place by management to mitigate identified risks (IIA, 2013b: 2).

The position and role of accountants and internal auditors in the financial services necessitates a proactive approach by initiating and monitoring organisational controls to expose money laundering and any other forms of corruption (Mulig & Murphy, 2004: 22).

7.6.3. Staff Capabilities and Organisational Needs

As highlighted by Hopton (2006: 3), those assigned the responsibility of recognising money laundering may have insufficient knowledge to enable them to identify it in all its disguises. This may be because money laundering has been inadequately defined.

However, internal auditing staff have industry specific knowledge ranging from financial reporting skills to IT security and other important abilities. In some instances, work can be outsourced as needed. When skills are required consistently throughout planning and implementation, the staff may need to undergo training (Martin, 2013: 32).

Internal auditing requires operational skills that traditional accountants or auditors may not have (Whitehouse, 2013a: 30). Mulig and Murphy (2004: 25) point out that the professional skills and expertise of internal auditors enables them in the fight against money laundering. The development of internal policies, procedures and controls to prevent money laundering falls within the accounting and auditing profession responsibilities.

7.6.4. The Risk-Based Approach followed by Internal Auditors

The risk-based approach championed by the IIA international Standards is an effective way to ensure that the priorities of the internal audit activity are consistent with the organisation's goals. Such an approach provides internal auditors with the

opportunity to become closely acquainted with the organisation's risk exposure and risk tolerance level (IIA, 2013b: 3).

The King III Report (Institute of Directors in Southern Africa, 2009: 14) argues that a compliance-based approach to internal auditing adds little value to the overall governance of an entity as it merely assesses compliance with existing procedures and processes without an evaluation of whether or not the procedure or process is an adequate control. The report states that a risk-based approach is more effective as it allows internal auditors to determine whether controls are effective in managing the risks which arise from the strategic direction that a company, through its board, has decided to adopt.

If an AML programme is risk-based, auditing procedures should focus on areas that present the greatest vulnerabilities (Risk Solutions Financial Services, 2007: 8-9). Although a full internal AML audit typically occurs annually, the frequency and scope of the compliance testing and BSA/AML audits can vary based on the institution's risk assessment. Business areas considered to have higher levels of inherent risk will require more comprehensive and frequent AML audits than those considered as low-risk (Axelrod & Ross, 2012: 73).

Internal audits should be risk-based but will vary depending on the bank's size, complexity, risk profile, quality of control functions, geographic diversity and use of technology. By incorporating the bank's BSA/AML risk assessment into the independent testing process, the audit programme can be more effectively tailored to cover all of the bank's activities (FDIC, 2008).

The internal auditing department is ideally suited for such a role as internal auditors are generally experts in risk assessment and internal control evaluation including control compliance monitoring. Furthermore the department is often organisationally independent with a direct reporting line to the board of directors and audit committee (Ligthtle & Bushong, 2000: 41).

Rossiter (2007: 34) points out that internal auditing today continuously refines risk identification and assessment capabilities. It enhances risk-based auditing by providing assurance and advice where it is most needed. Internal auditing aligns its activities with key business risks, recognising that auditing covers a range of activities regarding an entity's major risks. Internal auditors need to ensure that they are well positioned to manage and control emerging risks in future (Betts, 2008: 74).

In addition to their core responsibility of assessing and recommending internal controls, internal auditors' skills in risk management and their well-rounded perspective of an organisation makes them a unique and valuable resource regarding sound corporate governance. Informed senior managers and directors rely on internal auditors for advice and counsel on many issues including operational analysis risk assessment and improved corporate governance. When it comes to adding value to a business, internal auditing is one of the best resources (IIA, 2013b: 5).

7.7. Summary

Money laundering poses an immense challenge to the stability, integrity and reputation of the financial sector and through the process of globalisation and the increasing mobility of capital these threats have intensified (Ganguli, 2010:1).

Internal auditors can help detect and deter money laundering and terrorist financing activities as forms of fraud (Sinason et al., 2003: 11). This chapter provides an overview of internal auditing. It is explained as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" (IIA, 2013a).
The roles played by internal auditing include providing assurance and consultancy. Thus an understanding of the role of internal auditing in an organisation has been achieved.

The research provides a view of money laundering from a compliance risk and internal auditing perspective. The enterprise risk management process enables auditors to consider corruption risks when developing their risk assessments, specifically regarding whether the organisation is in compliance with federal and international laws including those related to money laundering (IIA, 2012d: 29).

Lastly, the research argues why internal auditors are in a better position to provide independent assurance on AML controls. A number of views are expressed which explain why internal auditing is better suited to provide assurance for AML compliance.

CHAPTER 8

CONCLUSION AND RECOMMENDATIONS

This chapter summarises the results of the literature study and proposes recommendations with reference to the initial research questions posed in the introduction. It informs the reader of discoveries, their value and deductions that can be made from the study as a whole. The conclusion generally contains four distinct sections including a summary of the findings, conclusions, contributions made by the study and suggestions for further research (Hofstee, 2009: 155, 157). This format will be followed here.

8.1. Conclusion

Due to the financial meltdown, the financial services sector saw a remarkable change in the policy design and implementation. Unsound financial systems were exposed and identified as a site for criminal activities (Shehu, 2010: 141). Prior to the financial crisis, the shocking events of 9/11 played a role in changing financial systems. At that point the AML sphere began a transformation. The link between money laundering and terrorist financing was detected (Pasley, 2011: 40).

Historic developments occurred including the improvement of coordination between government and the private financial sector, enhanced intelligence gathering and the establishment of significant AML requirements for banks, specifically regarding CFT. The passing of US Patriot Act in 2001 was also an important landmark in AML history (Pasley, 2011: 40). The 9/11 events signalled the beginning of a stricter international finance regime and a vast increase in obligations arising from various AML/CFT legal instruments (Leong, 2007: 150).

The culture of AML compliance was adopted to meet the AML challenges (Cromhout, 2002: 5). AML compliance regimes proposed and recommended practices such as KYC/CDD, suspicious transaction reporting and record keeping which assist in addressing the problem.

However, the compliance efforts to curb money laundering globally and the number of reported incidents of misconduct in financial indicate that more needs to be done to fight the problem. The research thus considered the role of independent AML compliance reviews and suggests this as a means to further the AML/CFT goals.

The first premise of the research was to illustrate that there is a general AML compliance challenge worldwide, whether it is from a cost versus benefit perspective non-compliance by financial institutions or regarding implementation. These challenges should not be ignored.

In keeping with international standards, financial institutions are required to build compliance functions to ensure that the business and its employees obey the applicable laws (De Koker, 2006: 38). Other dimensions such as regulatory and government effectiveness are critical to the quality of compliance (Hardouin, 2011: 151).

The research then proceeds to answer the question: “Is there a need for independent AML compliance reviews? The question revolves around the value of independent AML reviews.

Axelrod and Ross (2012: 73) state that independent annual audits or other forms of independent testing are pre-emptive safeguards against negative regulatory examination findings. Furthermore, the degree of integration and cooperation between the compliance department, internal auditing and the other business functions is often the key to AML programme success.

Thus, it is reasonable to deduce that independent testing provides assurance that the systems in place to manage the risk of non-compliance are operating efficiently and effectively.

The second part of the research considers the views expressed by leading practice authorities on independent testing. Both the FATF and US AML regimes promote independent reviews while South Africa was highlighted as deficient in this aspect.

In an integrated analysis of the South African money laundering problem, a comparison was made with the situation in other countries. The FATF Recommendations and best practice guidelines were reviewed and considered in terms of their practical application. Certain gaps were identified in this way and recommendations will be made in the next section to address the shortcomings. In the South African FIC Act, independent, internal audit functions or independent AML reviews are not considered a priority (De Koker, 2012: Com 6-6).

To provide a balanced literature review the position of the UK and the EU were also considered. However, the EU Directives and the JMLSG guidance contain no explicit recommendations on independent AML reviews (Delston, 2007: 6). In some instances these two regimes were vague. The use of words such as “appropriate” in these guidelines does not plainly communicate the need for independent AML reviews.

Despite the uncertainty regarding the EU and UK stance, there appears to be a need for independent AML compliance reviews as expressed by the FAFT and the US. The FATF has played an important role internationally in AML compliance and their recommendations on the need to ensure that financial institutions have an independent audit function to test the system should not be overlooked (FATF, 2012: 78). The US AML regime is among the leading, if not the best AML regime in the world, and their views on independent AML reviews are worth serious consideration.

8.2. Recommendations

The overall recommendation is that AML independent reviews and tests are an essential component in AML compliance challenge. AML compliance is paramount but an independent AML compliance review provides an additional safeguard to ensure that the AML processes in place are working as intended.

The main objective of the independent review is to provide a fair and unbiased assessment of the organisation's AML programme. The review should include internal control tests, procedures to identify control breakdowns and weaknesses and recommendations to management regarding appropriate corrective actions that will mitigate money laundering risks (Department of the Treasury, 2006: 2-3).

Other important recommendations are made regarding the objectives of the study. One of these objectives deals with determining the appropriate frequency of independent reviews. Although there are many views on this, the most noteworthy recommendation is that independent reviews should be conducted based on a risk assessment that considers the business' products, services, customers and geographic locations. The risk assessment would then inform both the frequency and scope of the AML independent reviews (Department of the Treasury, 2006: 2-3).

Another objective sought to identify who is well positioned to provide an independent review. As discussed previously, because compliance monitoring is a continuous process by design, ensuring that business is conducted in accordance with the applicable regulatory requirements is a priority and internal auditing is viewed as having a critical role to play. In the context of compliance, the internal auditor's role is to ensure that the compliance process is operating effectively (Terblanché et al., 2008).

Axelrod and Ross (2012: 72) highlight that the US Patriot Act of 2001 requires relevant personnel inside or outside an institution to carry out annual independent tests of the AML programme. Their argument raised shows that internal auditors are generally considered to have the adequate independence to perform this role.

Beaumier (2005/2006: 31) argues that the responsibility of ensuring that the bank's AML programme is effective is a shared responsibility. However, a critical success component of the AML programme is the internal audit or another independent third party review that is charged with the responsibility of conducting independent tests. Internal auditors can help detect and deter money laundering and terrorist financing activities (Sinason et al., 2003: 11). Independent testing by knowledgeable internal

auditors is critical to ensuring that AML/CFT programmes are fully aligned with regulatory requirements (Khan, 2007: 46).

The research shows that internal auditors can perform independent AML reviews, primarily because of their degree of independence. Internal auditing operates separately from the compliance and other business functions and is able to provide unbiased recommendations that add value to the AML programme. Other benefits offered by internal auditors include their understanding of risk and risk management processes (through a risk-based AML approach and risk-based auditing), understanding controls (in terms of action plans to mitigate and minimise money laundering) and their various capabilities and skills.

8.3. Suggestions for Future Research

This section may be slightly contentious in that it addresses areas not covered in the research but are related to the topics considered. When proposing a sound argument further, related often questions arise and it is in this way that new research is developed (Hofstee, 2009: 162).

Hofstee (2009: 162) points out that when identifying areas for further research, the suggestions made should allow the next scholar to undertake similar work but using other (possibly newer) methods, investigate questions brought to the fore by current research or use the current research in other related areas.

A research study is not an isolated intellectual activity isolated from other similar studies but it adds to previous research and acknowledges that other research will take place in the foreseeable future in the same field (Oliver, 2004: 156). For that reason, listed below are the potential areas for further research.

8.3.1. The Role of the Legal Profession and Other Professions in Performing Independent AML Reviews

The New FATF Recommendations, particularly Recommendation No. 18, require the AML/CFT programmes in financial institutions to include an independent audit

function to test the system (FATF, 2012: 77) but it is not clear who should perform the AML independent review.

Through the research study conducted, recommendations are made that favour internal auditing. However, as expressed in section 1.8 on limitations, the research argues mainly from an internal auditing viewpoint but does not imply that internal auditors are the only professionals equipped to perform an independent review. Further research could argue whether the legal profession or any other profession is suited to the work. Direct comparisons can be drawn between other professions and internal auditing in performing independent AML reviews.

8.3.2. Who Should the Independent AML Audit Function Report To and why?

The idea of an independent AML audit has been argued at length in the research however in answering one question the research has created another question. In line with the theme, and to ensure a consistent AML compliance programme of value, the following question arises: “Who should the function performing the independent AML review report to and why?”

Generally there appears to be confusion about the role of the compliance function versus the role of risk management and this may also be considered (Sharon, 2006: 12).

Delson (2007: 6) argues that independence means not just being outside the AML teams that implement a programme but it also requires a different reporting line. It also should not involve the responsibility of drafting and implementing the company AML programme. Shonk’s (2007a: 8) viewpoint is that AML audits cannot be performed by individuals administering the AML programme or those supervised by the compliance officer. This means that AML independence should be recognised and understood.

With that said, a key area worth researching is where should the independent audit function report to and why. It one thing to have in an independent audit to review

AML systems in place, it is equally crucial to understand where this function should reports to? Important issues to consider are role conflicts, such as when the auditor must report to a compliance officer, how to ensure that compliance officers are accountable for instances of non-compliance or gross negligence and challenging various ineffective AML practices.

8.3.3. The Lack of Skills, Qualification and Experience Clarity on the Requirements for Independent AML Reviewers

Although independent audits have now been incorporated as an AML priority by the FAFT, there is still no clarity as to who must perform these reviews. Although this has been partly addressed as part of the research, a number of creditable authors have proposed who should perform independent AML reviews.

Beaumier (2005/2006: 31) points out that individuals performing independent reviews must be adequately qualified, have knowledge of the legal and regulatory requirements, a sound understanding of a financial institution's customer base including its products and services.

This brings us to the next question. Given the complex nature of the criminal activities involved in money laundering, what skill set and expertise would be required to perform an independent money laundering review that would provide senior management and the board with an adequate level of assurance that the money laundering risk is being adequately and effectively managed

That said, the FATF viewpoint gives no clear indication of the skills, qualifications and experience required for the designated individual who performs independent AML reviews. It is essential that this area of potential research be pursued in order to ensure that value can be derived from independent AML reviews

REFERENCES

Agarwala, G., Girling, A. & Makol, N. 2008. Meeting the internal audit challenges of Basel 2. *Internal Audit* , May/June: 25–29.

Angel, I.O. & Demitis, D.S. 2005. System thinking about anti-money laundering: Considering the Greek case. *Journal of Money Laundering Control*, 8(3): 271–284.

Anonymous. 2007. Creating compliance programs for casinos: Anti-money laundering regulations. *Journal of Macao Polytechnic Institute*, 17–18.

Anonymous. 2008. FDIC highlights importance of independence testing for BSA/AML compliance. *Bank Auditing and Accounting Report*, June: 2–4.

Axelrod, R.M. & Ross, K. 2012. Effective AML compliance. *Internal Auditor,* August: 71–73.

Banda, J., Munyoro, J., Goba, R., Fundira, B., Goredema, C. & Capito, B. 2007. *Confronting the proceeds of crime in Southern Africa.* Pretoria: Institute for Security Studies.

Beach, L.A. 2006. Making the change to continuous auditing. *IIA IA Adviser,* July: 11–13.

Beaumier, C. 2005/2006. Auditing anti-money laundering compliance. *Bank Accounting and Finance,* December/January: 31–34.

Beaumier, C. & Shah, S. 2003. Anti-Money Laundering Compliance. *ABA Compliance*, November/December 24(11): 12–17.

Beekarry, N. 2011. The international anti-money laundering and combating of financing terrorism regulatory strategy: A critical analysis of compliance determinants in internation law. *Northwestern Journal of International Law and Business*, 137–193.

Betts, N. 2008. Internal audit: Who's in control. *New Zealand Management*, February, *55*(1): 74–75.

Biegelman, M.T. & Bartow, J.T. 2006. *Executive roadmap to fraud.* New Jersey: John Wiley.

Binneman, D. 2012. Reputational risk, years to build and seconds to destroy. *IIA IA Adviser,* October: 33–37.

Bryne, J.J. & Kelsey, M.D. 2006. AML enforcement actions. *ABA Bank Compliance,* May/June: 8–13.

Burnaby, P. & Hass, S. 2004. Trends in internal audit strategies. *Internal Audit*, May/June: 15–21.

Chan, C. 2009. Available at http://ar.cetl.hku.hk/index.php. Accessed on 21 October 2013, from ar@hku: http://ar.cetl.hku.hk/am_literature_reviews.htm

Christopher, J., Sarens, G. & Leung, P. 2009. A critical analysis of the independence of internal audit function: Evidence from Australia. *Accounting, Auditing and Accountability Journal*, 22(2): 200–220.

Commonwealth Secretariat. 2006. *Combating money laundering and terrorist financing: A model of best practice for the financial sector, the professionals and other designated business.* 2nd edition. London: Commonwealth Secretariat.

Costanzo, C. 2008. AML on the outside. *Community Banker,* June: 24–27.

Cox, D. 2011. *An introduction to money laundering deterrence.* 1st edition. Chichester, West Sussex: John Wiley.

Cromhout, P. 2002. Cleaning up SA's act. *Accountancy SA,* August: 5.

De Kock, A., Kruger, N., Roper, P. & Odendaal, H. 2002. *The practical guide to offshore investments.* Brooklyn: Offshore Investments Corporation.

De Koker, L. 2002a. Money laundering in South Africa. *Journal of Money Laundering Control*, 6(1): 166–181.

De Koker, L. 2002b. Money laundering trends in South Africa. *Journal of Money laundering Control*, 6(1): 27–41.

De Koker, L. 2006. Money laundering control and suppression of financing of terrorism. *Journal of Financial Crime*, 13(1): 26–50.

De Koker, L. 2009. The money laundering risk posed by low-risk financial products in South Africa. *Journal of Money Laundering Control*, 12(4): 323–339.

De Koker, L. 2012. *South African money laundering and terror financing law.* Durban: Lexis Nexis.

Delston, R. 2007. Independent AML audit: Essential element or nice to have. *Money Laundering Bulletin,* June: 5–9.

Delston, R.S. & Walls, S.C. 2009. Reaching beyond banks: How to Target trade-based money laundering and terrorist financing outside the financial sector. *Case Western Reserve Journal of International Law,* Cleveland.

Department of the Treasury. 2006. *Frequently asked questions: Conducting independent reviews of money services business anti-money laundering programs.* Available on: http://www.fincen.gov/search/search?q=independent+aml+reviews&entqr=0&ud=1&sort=date%3AD%3AL%3Ad1&output=xml_no_dtd&oe=UTF-8&ie=UTF-8&client=www_redesign&proxystylesheet=www_redesign&site=www_fincen_gov Accessed 27 March 2013.

De Smet, D. & Mention, A. 2011. Improving auditor effectiveness in assessing KYC/AML practices. *Managerial Auditing Journal*, 26(2): 182–203.

Dinga, G.R. 2012, October. Combined Assurance in the public sector. *IIA IA Adviser*, 16–17.

Dollar, B. & Shughart, W.F. 2011. Enforcement of the USA Patriot Act's anti money laundering provision: Have regulators followed a risk-based approach? *Global Finance Journal,* Vol 22: 19–31.

Dollar, B. & Shugart, W.F. 2012. The USA Patriot Act's differential impact on large and small banks: Evidence from California's high-risk money laundering and related financial crime areas. *Journal of Banking Regulation*, 13(2): 127–146.

Egmont Group. 2004. *Egmont Group.* September. Available at www.egmontgroup.org/library/download/3 Accessed 2 March 2012.

Federal Deposit Insurance Corporation (FDIC). 2008. *Federal Deposit Insurance Corporation*. Available from http://www.fdic.gov/news/news/financial/2008/fil08038.html Accessed 21 June 2013.

Financial Action Task Force (FATF). 2003a. *Financial Action Task Force on Money Laundering: Annual review of non-cooperative countries or territories.* Paris: FATF Secretariat .

Financial Action Task Force (FATF). 2003b. *Financial Action Task Force on Money Laundering: The Forty Recommendations.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2004. *South Africa: Report on observance of standards and codes, FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2007. *Guidance on the Risk-based approach and terrorist financing: High-level principles and procedures.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2009b. *Mutual evaluation report: Anti-money laundering and combating the financing of terrorism South Africa.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2010a. *An introduction to the FATF and its work.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2010b. *FATF*. Available at http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html Accessed 7 February 2012.

Financial Action Task Force (FATF). 2011. *FATF Public Statement, February 2011*. Available at http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement-25february2011.html Accessed 24 July 2013.

Financial Action Task Force (FATF). 2012. *International Standards combating money laundering and the financing of terrorism and proliferation: The recommendations.* Paris: FATF Secretariat.

Financial Action Task Force (FATF). 2013. *Methodology for assessing compliance with the FAFT recommendations and the effectiveness of AML/CFT systems.* Paris: FATF Secretariat.

Financial Crimes Enforcement Network. n.d. *The Hawala Alternative remittance system and its role in money laundering.* Vienna: Financial Crimes Enforcement Network.

Financial Intelligence Centre (FIC). 2001. *Financial Intelligence Centre Act* February. Pretoria: FIC.

Financial Intelligence Centre (FIC). 2006. Consultation document: Proposed Amendments to the Financial Intelligence Centre Act 2001. FIC Act No. 38 of 2001. August. Pretoria: FIC.

Financial Intelligence Centre (FIC). 2006/2007. *Financial Intelligence Centre Annual Report.* Pretoria: FIC.

Financial Intelligence Centre (FIC). 2009/2010. *Annual Report 2009/2010.* Pretoria: FIC.

Financial Intelligence Centre (FIC). 2010. Amendments of schedule 1 of the Financial Intelligence Centre Act No. 38 of 2001. November. Pretoria: FIC.

Financial Intelligence Centre (FIC). 2010/2011. *Summary report on Financial Intelligence Centre.* Pretoria: FIC.

Financial Intelligence Centre (FIC). 2011/2012. *Increasing collaboration to strengthen financial integrity: Financial Intelligence Centre Annual Report 2011/2012.* Pretoria: FIC.

Financial Intelligence Centre (FIC). 2012. *Preventing and suppressing terrorist financing.* Available from

http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/spmtg_south_africa20nov12.pdf Accessed 7 February 2013.

Financial Services Authority (FSA). 2007. A glossary of terms relevant to the Money Laundering Regulations 2007. *Money Laundering Regulations* October. London, UK: FSA.

Financial Services Authority (FSA) 2012. *FSA*., Available from http://www.fsa.gov.uk/about Accessed 5 September 2012.

Ford, W. 2003. Money laundering. *IIA IA Adviser,* August: 10–11.

Gallant, M.M. 2005. *Money laundering and the proceeds of crime: Economic crime and civil remedies.* Cheltenham: Edward Elgar.

Galvan, J.L. 2006. *Writing Literature reviews: A guide for students of the social and behavioral sciences.* 3rd edition. Glendale: Pyrczak.

Ganguli, I. 2010. The third directive: Some reflections on Europe's new AML/CFT regime. *Banking and Financial Services Report,* May, 29(5): 1–18.

Gao, S., Xu, D., Wang, H. & Wang, Y. 2006. *Intelligent anti-money laundering system.* Hong Kong: University of Hong Kong.

Garbutt, J. 2011. Internal audits key to thwarting money launderers. *Asset Management*, June, Vol. 125: 31–33.

Garces, I. 2010. Considering a bank acquisition? Don't forget BSA and AML. *Bank Director*, 58.

Gardner, K.L. 2007. *Fighting terrorism the FAFT way.* Lynne Reiner.

Geary, J.M. 2009. Light is the best antidote. *Journal of Money Laundering*, 12(3): 215–220.

Geiger, H. & Wuensch, O. 2007. The fight against money laundering: An economic analysis of costs-benefit paradoxes. *Journal of Money Laundering Control*, 10(1): 91–105.

Geister, D. 2010. *Concepts in customer due diligence: Meeting the challenge of regulatory expectations.* California: LexisNexis.

Goredema, C. 2006. *Money laundering survey in East and Southern Africa: January to June 2006.* Pretoria: Institute of Security Studies.

Goredema, C. 2007. *Confronting the proceeds of crime in Southern Africa.* Pretoria: Institute for Security Studies.

Goredema, C. 2012. *Institute for Security Studies.* Available from http://www.issafrica.org/iss_today.php?ID=1455 Accessed 25 January 2013.

Government of South Africa. 2009. Companies Act. *Government Gazette*.

Hardouin, P. 2011. The aftermath of the financial crisis. *Journal of Financial Crime*, 18(2): 148–161.

Harrington, C. 2004. Internal audit's new role. *Journal of Accountancy*, 65–70.

Helgesson, K.S. & Morth, U. 2012. *Transforming the public security domain.* Abingdon: Routledge.

HM Treasury. 2007. *The financial challenge to crime and terrorism.* London: HMSO.

Hofstee, E. 2009. *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule.* Sandton: EPE.

Hopton, D. 2006. *Money laundering: A concise guide for all business.* Hampshire: Gower.

Hübschle, A. 2010. *Organised crime in Southern Africa: First annual review.* Pretoria: Institute of Security Studies.

Husisian, G. 2010. Coping with US regulations of international conduct: Anti money-laundering and compliance. *Insights*, 24(1).

Independent Regulatory Board of Auditors (IRBA). 2011. *A guide for registered auditors: Combating money laundering and financing of terrorism.* Modderfontein: IRBA.

Institute of Directors in Southern Africa. 2009. *King Code of Governance for South Africa.* Johannesburg: Institute of Directors in Southern Africa.

Institute of Internal Auditors (IIA). 2001. *New guidance for the professional practice framework.* Florida: IIA.

Institute of Internal Auditors (IIA). 2004. *New guidance for the professional practice framework.* Florida: IIA.

Institute of Internal Auditors (IIA). 2005. Common misconceptions. *IIA IA Adviser* May, pp. 32-4.

Institute of Internal Auditors (IIA). 2006. Message for the IIA Inc's quality department. *IIA IA Adviser,* September: 38–41.

Institute of Internal Auditors (IIA). 2008. *iKutu research report.* Bedfordview: IIA.

Institute of Internal Auditors (IIA). 2010. *Internal Auditing SA*. Available from http://www.iiasa.org.za/technical-guidance/global-guidance/internal-auditing-definition.html Accessed 1 March 2012.

Institute of Internal Auditors (IIA). 2012a. *Independence and objectivity*. Available from https://global.theiia.org/standards-guidance/topics/Pages/Independence-and-Objectivity.aspx Accessed 21 May 2012.

Institute of Internal Auditors (IIA). 2012b. *2012 Integrated report.* Bedfordview: IIA.

Institute of Internal Auditors (IIA). 2012c. *International standards for professional practice of internal auditing: Standards.* Florida: IIA.

Institute of Internal Auditors (IIA). 2012d. Shining a light on corruption. *IIA IA Adviser*, October: 28–30.

Institute of Internal Auditors (IIA). 2013a. *About the profession*. Available from https://na.theiia.org/about-us/about-ia/pages/about-the-profession.aspx Accessed 23 April 2013.

Institute of Internal Auditors (IIA). 2013b. *Internal auditing: Adding Value across the board.* Available from https://na.theiia.org/about-

ia/PublicDocuments/Internal_Auditing-Adding_Value_Across_the_Board.pdf Access 23 April 2013.

International Monetary Fund (IMF). 2004. *South Africa: Report on the Observance of Standards and Codes on Banking Supervision, Insurance Supervision, and Securities' Regulation.* Washington DC: IMF.

International Monetary Fund (IMF). 2012. *International Monetary Fund*. Available from http://www.imf.org/external/np/exr/facts/aml.htm Accessed 5 September 2012.

Iovitu, M., Borisov, D., & Calanter, P. 2013. *The Internal Audit Function: Evolution and Role.* Bucharest: Bucharest Academy of Economy Studies.

Jakobi, A.P. 2012. The FATF as a central promoter of the anti money laundering regime. In *Securitization, accountability and risk management* edited by K.S. Helgesson & M. Ulrika. Abingdon: Routledge, 16–33.

Jensen, N. & Png, C.-A. 2011. Implementation of the FAFT 40 + 9 recommendations: A perspective from developing countries. *Journal of Money Laundering Control*, 14(2): 110–118.

Johnson, B.R. & Carrington, I. 2006. Protecting the financial system from abuse. *Journal of Money Laundering Control*, 9(1): 48–61.

Johnson, J. 2008. Is the global financial system AML/CFT prepared? *Journal of Financial Crime*, 15(1): 7–21.

Johnson, J. & Lim, D.Y. 2002. Money laundering: Has the Financial Action Task Force made a difference? *Journal of Financial Crime*, 10(1): 7–22.

Joint Money Laundering Steering Group (JMLSG). 2011. *Prevention of money laundering/combating terrorist financing: 2011 review version.* London: JMLSG.

Joint Money Laundering Steering Group (JMLSG). 2012. *Joint Money Laundering Steering Group*. Available from http://www.jmlsg.org.uk/ Accessed 15 August 2012.

Joubert, M. 2008. Internal audit planning. *IIA IA Adviser,* August: 13–28.

Julien, R. & Richards, T. 2008. Rising to the challenge: Internal auditors can play a strategic role in emerging ERM and governance programs. *Internal Auditor,* February: 43–44.

Khan, S.M. 2007. Tips for testing anti-money laundering programs. *Internal Auditor* October: 47–48.

Killick, M. & Parody, D. 2007. Implementing AML/CFT measures that address the risks and not tick boxes. *Journal of Financial Regulation and Compliance,* 15(2): 210–216.

Kincaid, J.K., Sampias, W.J. & Marcella, J.R.A.J. 2004. *CCSA control self-assessment.* IIA Research Foundation.

Kruger, A. 2008. *Organised crime and proceeds of crime law in South Africa.* Durban: Lexis Nexis.

Kumar, R. 2011. *Research methodology.* 3rd edition. London: Sage.

Leedy, P. & Ormrod, J. 2001. *Practical research: Planning and design.* 7th edition. New Jersey: Pearson Education.

Leong, A.V. 2007. Chasing dirty money: Domestic and international measures against money laundering. *Journal of Money Laundering Control*, 10(2): 140–156.

Ligthtle, S.S. & Bushong, G.J. 2000. The role of internal audit in the effort to improve audit committee effectiveness. *The Ohio CPA Journal*, 39–43.

Lister, L.M. 2007. A practical approach to Fraud risk. In *Internal auditor*. n.p., 61.

Machaba, S. 2012. Optimising your internal audit function. *IIA IA Adviser,* October: 10.

Maranto, M. 2006. Strengthening AML programs: The time is now, not tomorrow. *US Banker,* March: 56.

Marrelli, A.F. 2005. *Literature reviews.* Available from http://www.ispi.org/pdf/suggestedReading/ArticleFive_LiteratureReviews.pdf Accessed 7 August 2013.

Martin, A.G. 2013. A refocused internal audit function adds value. *Internal Auditing*, January/February: 25–34.

Mathers, C. 2004. *Crime school: Money laundering.* New York: Firefly Books.

Mills, A. 2008. *Essential strategies for financial services compliance.* Chichester: John Wiley.

Mohamed, S. 2002. Legal Instruments to combat money laundering in the EU financial market. *Journal of Money Laundering Control*, 6(1): 66–79.

Mont, J. 2012. *Compliance back in the spotlight*. July. Available from http://www.complianceweek.com/pages/login.aspx?returl=/aml-compliance-back-in-the-spotlight/article/250959/&pagetypeid=28&articleid=250959&accesslevel=2&expireddays=0&accessAndPrice=0 Accessed 20 June 2013.

Moshi, H.P. 2007. *Fighting money laundering: The challenges in Africa.* Pretoria: Institute for Security Studies.

Moss, V.Y. & Seabron, N. 2010. BSA compliance remains a challenge. *Credit Union Magazine*, January: 44–46.

Mouton, J. 2001. *How to succeed in your masters and doctoral studies.* Pretoria: Van Schaik.

Mugarura, N. 2011. The institutional framework against money laundering and its underlying predicate crimes. *Journal of Financial Regulation and Compliance*, 19(2): 174–194.

Mulig, E.V. & Murphy, S. 2004. Understanding and preventing money laundering. *Internal Auditing,* September/October: 22–25.

Muller, W., Kalin, C. & Goldsworth, G. 2007. *Anti-money laundering: International law and practice.* New York: Wiley.

Nevin, T. 2000. Has Africa become the world's washroom for dirty money? *African Business*, March: 20.

Okogbule, N.S. 2007. Regulations of money laundering in Africa: The Nigerian and Zambian approaches. *Journal of Money Laundering Control*, 10(4): 449–463.

Oliver, P. 2004. *Writing your thesis.* London: Sage.

O'Reilly, A. 2006. Money laundering: Transposing the Third AML Directive. *Accountancy Ireland,* April, 38(2): 59–61.

Osborne, P.R. 2006. Building a risk-based BSA/AML audit program. *ABA Bank Compliance*, November/December: 4–7.

Pallay, J. 2004. Analysing AML audits. *Wall Street & Technology,* August: 36–37.

Pasley, R. 2011. Ten years: What have we learned, how have we changed. *ABA Banking Journal*, 40–44.

Pieth, M. & Aiolfi, G. 2002. *Anti-money laundering: Levelling the playing field.* Basel: Basel Institute of Governance.

Ping, H. 2006. Lawyers, notaries and accountants and money laundering. *Journal of Money Laundering Control*, 9(1): 63–70.

Ping, H. 2008. The measures on combating laundering and terrorism financing in the PRC. *Journal of Money Laundering Control*, 11(4): 320–330.

PriceWaterhouseCoopers (PwC). 2010. *Independent review of anti-money laundering/anti-terrorist financing compliance policies and procedures.* Available from http://www.pwc.com/ca/en/risk/forensic-services/anti-money-laundering-anti-terrorist-financing-review.jhtml Accessed 26 March 2013.

Public Accountants and Auditors Board. 2003. *Money laundering: A guide for Registered accountants and auditors.* Johannesburg: Public Accountants and Auditors Board.

Qorchi, M., Maimbo, S. & Wilson, J. 2003. *Informal funds transfer systems: An analysis of the informal Hawala system.* Washington DC: IMF.

Raghavan, K.R. 2006. Intergrating anti-money laundering into compliance structure. *Bank Accounting and Finance,* October/November: 29–44.

Rezaee, Z. 2002. *Financial statement fraud.* New York: John Wiley.

Richards, J.R. 1999. *Transnational criminal organisations, cyber crime, and money laundering: A handbook for law enforcements officers, auditors, and financial investigators.* Florida: CRC Press.

Risk Solutions Financial Services. 2007. *Practical USA Patriot Act: Principles for banks and financial institutions.* Irvine, CA: LexisNexis.

Risk Solutions Financial Services. 2010. *Emerging anti-money laundering risk to financial institutions.* Irvine, CA: LexisNexis.

Ross, S. & Hannan, M. 2007. Money Laundering regulation and risk based decision making. *Journal of Money Laundering Control*, 10(1): 106–115.

Rossiter, C. 2007. Top 10 Priorities for internal audit in a changing environment. *Bank Accounting & Finance,* August/September, 20(5): 34–38.

Rowley, J. & Slack, F. 2004. Conducting a literature review. *Management Research News*, November, 27(6): 31–39.

Salih, C. 2011. Banks warned to turn away money laundering risks or face FSA action. *Money Marketing*, June: 23–24.

South African Reserve Bank (SARB). 1996. *The Banks Act No. 94 of 1990*, *As Amended.* Pretoria: SARB.

South African Reserve Bank (SARB). 2002. *Bank Act.* Available from http://www.resbank.co.za/RegulationAnd Supervision/BankSupervision/BankingLegislation/Pages/BankAct.aspx Accessed 22 April 2012.

Sartip, A. 2008. Auditing the integrity of AML programs. *Internal Auditor,* February: 55–58.

Schneider, F. & Windischbauer, U. 2010. *Money laundering: Some facts.* Berlin: German Institute for Research (DIW Berlin).

Scholtz, J. & De Villiers, D. n.d. Available from www.webberwentzel.com: www.webberwentzel.com/wwb/action/media/downloadFile?media... Retrieved 7 February 2013.

Seyad, S.M. 2012. The EU anti-money laundering legal regime. In *Securitization, accountability and risk management* edited by K.S. Helgesson & M. Ulrika. Abingdon: Routledge, 34–55.

Shanmugan, B. 2004. Hawala and money laundering: The Malaysian perspective. *Journal of Money Laundering Control*, 37–47.

Sharon, B. 2006. Operational risk management: The difference between risk management and compliance. *Business Credit,* July/August: 12.

Shehu, A.Y. 2010. Promoting financial sector stability through an effective AML/CFT regime. *Journal of Money Laundering Control*, Vol. 2: 139–154.

Shonk, K. 2007a. Tools for managing AML compliance risk. *Regulatory Report*, January pp. 7-10.

Shonk, K. 2007b. Know your customer: ATM transactions may indicate money laundering. *Community Banker*, April, 16(4): 56–57.

Simonova, A. 2011. The risk-based approach to anti-money laundering: Problems and solutions. *Journal of Money Laundering Control*, 14(4): 346–358.

Sinason, D., Pacini, C. & William, H. 2003. The internal auditor's role in fighting terrorist financing. *Internal Auditing*, March/April: 11–18.

South African National Treasury. 2013. *Budget speech.* Pretoria: South African National Treasury.

Sproat, P.A. 2009. To what extent is the UK's anti-money laundering and asset recovery regime used against organised crime. *Journal of Money Laundering Control*, 12(2): 134–150.

Stikeman, E. 2013. *UK implements "twin peaks" model of financial regulation*. April. Available from http://www.lexology.com/library/detail.aspx?g=98c9c22a-63e4-4852-abd9-6210168a21b7 Accessed 15 December 2013.

Steinberg, R. M. 2005. What risk and compliance officers should be doing. *IIA IA Adviser*, March: 20–21.

Tabuen, J. 2013. Where internal audit and compliance should report. *Compliance Week*, February: 28–29.

Tavares, C., Thomas, G. & Roudaut, M. 2010. *Money laundering in Europe: Report of work carried out by EuroStat and DG Home Affairs.* Luxembourg: EU.

Temporary Cease and Desist Order, SEC-2010-82 (Commissioner of Securities and Insurance Office of the state auditor, State of Montana August 2, 2010).

Terblanché, J., Van der Merwe, R. & Schlebusch, C. 2008. *Accountancy SA* June. Available from http://www.accountancysa.org.za/resources/ShowItemArticle.asp?ArticleId=1466&Issue=1010 Accessed 17 July 2013.

US Department of Homeland Security. n.d. *US Immigration and customs enforcement*. Available from http://www.ice.gov/cornerstone/money-laundering.htm Accessed 16 May 2011.

UK Treasury. 2003. *Managing the risk of fraud: A guide for managers.* London: UK Treasury.

Unger, B. 2007. *The scale and impacts of money laundering.* Cheltenham: Edward Elgar.

UNODC. 2011. *Estimating illicit financial flows resulting from drug trafficking and other transactional organised crime.* Vienna: United Nations Office on Drugs and Crime.

US Department of the Treasury. 2006. *Conducting independent reviews of money services business and anti-money laundering programs.* Washington DC: Financial Crimes Enforcement Network.

US Government. 2001. US Patriot Act 2001. *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism*. October USA: US Government.

US State Bureau for International Narcotics and Law Enforcement Affairs. 2012. *International Narcotics Control Strategy Report.* Washington DC: US Bureau for International Narcotics and Law Enforcement Affairs.

Van den Broek, M. 2011. The EU's preventive AML/CFT policy: Asymmetrical harmonisation. *Journal of Money Laundering Control*, 170–182.

Van de Westhuizen, M. 2008, July. Suspicious transaction reporting in terms of s 29 of FICA. *De Rebus*, 30–31.

Veazie, J. 2011, July. The role of internal audit. *Health Care Collectors*, 25(2): 9–12.

Verhage, A. 2008. *Between the hammer and the anvil? The anti-money laundering complex and its interactions with compliance industry.* Ghent: Springer.

Verhage, A. 2009. Compliance and AML in Belgium: A booming sector with growing pains. *Journal of Money Laundering Control*, 12(2): 113–133.

Von Eck, C. 2011. More being asked of internal auditors than before. *Business Report,* December: 6.

Von Eck, C. 2012. *Independence is a state of mind*. April. Available from http://www.iiasa.org.za/component/k2/item/6-independence-is-a-state-of-mind.html Accessed 21 May 2012.

Whitehouse, T. 2013a. Internal audit teams facing rapid changes in 2013. *Compliance Week,* January: 30–31.

Whitehouse, T. 2013b. IA focusing on compliance risk: Streamline testing. *Compliance Week*, May: 10.

Wolfsberg Group. 2006. *Guidance on a Risk based for managing money laundering risks.* Basel: Wolfsberg Group.

Wolfsberg Group. 2011. *Wolfsberg principles*. Available from http://www.wolfsberg-principles.com/ Accessed 21 April 2012.

Yasin, N.M. 2004. Lawyers, legal privilege and money laundering: The UK and Malaysian experience. *Journal of International Banking Regulation*, 5(4): 364–386.

Zagaris, B. 2007. Problems applying traditional anti-money laundering procedures to non-financial transactions, 'parallel banking systems' and Islamic financial systems. *Journal of Money Laundering Control*, 10(2): 157–169.

Zhu, M. 2012, March. *International Monetary Fund*. Available from http://www.imf.org/external/np/exr/facts/aml.htm Accessed 5 September 2012.