

A TECHNICAL ASSESSMENT OF CERTAIN SAUDI ARABIA LAWS, REGULATIONS, AND INSTITUTIONS

Excerpts of a December 2003 review of the new Saudi Arabian legal, regulatory, and institutional regime to combat money laundering and terrorist financing, commissioned by, and presented to, the Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations.

Methodology

The report's analysis is divided into three chapters: Criminal Law, Regulatory Regime, and International Cooperation. The Criminal Law chapter assesses the criminalization of money laundering and terrorist financing in Saudi Arabia, and the agencies charged with enforcing these provisions. The Regulatory Regime evaluates the regulatory framework in Saudi Arabia as applicable to the financial, commercial and non-profit sectors, with a brief overview of the "informal" sector. Finally, the International Cooperation chapter addresses the mechanisms and procedures that Saudi Arabia has put in place for coordination of its anti-money laundering and combating terrorist financing (AML/CTF) efforts with those of other jurisdictions.

Each chapter contains sub-chapters, which represent independent themes within that chapter. For example, the Criminal Law chapter is divided into Scope of Money Laundering Offense, Scope of Terrorist Financing Offense, Sanctions, Designation of Authorities, and Capacity of Authorities. Each sub-chapter, is divided into a number of principles relevant to assessing Saudi Arabia's compliance with international standards and relating to that sub-chapter's theme. For example, the Sanctions sub-chapter within Criminal Law chapter contains the principle - Confiscating and Attaching Terrorist Assets.

Many, though not all of these principles are drawn from the Financial Action Task Force's "40 Recommendations on Money Laundering" and its "8 Special Recommendations on Terrorist Financing."

For each principle, we assessed Saudi Arabia’s compliance from a legal perspective, an enforcement perspective, and an implementation perspective. The legal perspective examined the relevant Saudi laws and regulations, and evaluated their soundness and thoroughness. The enforcement perspective examined the governmental authorities charged with enforcing these laws and regulations, and evaluated their enforcement activity. The implementation perspective examined the persons and entities subject to the laws and regulations, and evaluated the impact on their conduct. Not all perspectives are relevant to each principle.

The documentary evidence we compiled included both primary sources, consisting of Saudi laws and regulations, and secondary sources, such as Congressional testimony, treatises by legal scholars, and news reports. In addition, we interviewed various persons with relevant banking, legal or other expertise.

As part of our effort to conduct a professional-caliber analysis of the laws, regulations, institutions and practices of Saudi Arabia, in early October we sent a detailed request for information and documents on these topics to the Saudi Arabian Foreign Policy Advisor, Mr. Adel Al-Jubeir. Unfortunately, we did not receive any documents or information in response to this request.

Wherever applicable, we based our analysis of Saudi Arabia’s AML/CTF efforts on relevant international standards, in accordance with the FATF Recommendations. These standards included:

- 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (“The Vienna Convention”)
- 1999 International Convention for the Suppression of the Financing of Terrorism
- 2000 United Nations Convention Against Transnational Organized Crime (“The Palermo Convention”)
- 2001 UN Security Council Resolution 1373
- 1999 Basel Committee on Banking Supervision Core Principles and Methodology (“The Basel Principles”)
- 2002 FATF Best Practices Guidelines on Combating the Abuse of Non-Profit Organization (The “FATF NPO Guidelines”)

- Egmont Group Financial Intelligence Unit Definition
- Corporate best practices from leading financial institutions
- Basel Customer Due Diligence Guidelines

Criminal Law

A vital component of a country's anti-money laundering and combating terrorist financing (AML/CTF) effort is its criminalization of the core conduct of money laundering and terrorist financing. Such criminalization brings to bear the investigative resources of the criminal law enforcement authorities, as well as the deterrence effect of criminal sanctions. In addition, the thoroughness with which a country criminalizes ML/FT activity sends an important public message about its determination to eradicate such activity, while stigmatizing and delegitimizing those who engage in it.

This chapter will examine the criminal law component of Saudi Arabia's AML/CTF effort along five vectors:

- Scope of Money Laundering Offense: The adequacy of the legal scope of money laundering as a criminal offense, including the definition of money laundering, the associated mental state requirement, and the extension of money laundering criminal liability to legal persons.
- Scope of Terrorist Financing Offense: The adequacy of the legal scope of terrorist financing as a criminal offense, including the definition of terrorist financing, the associated mental state requirement, and the extension of terrorist financing criminal liability to legal persons.
- Sanctions: The adequacy of criminal sanctions against natural or legal persons that engage in money laundering or terrorist financing, including both pre-trial attachment of suspect assets and post-conviction imprisonment, confiscation and other criminal penalties.
- Designation of Authorities: The adequacy of the formal designation and legal empowerment of law enforcement authorities charged with enforcing the criminal law AML/CTF provisions, including their authority to demand and obtain evidence and information.
- Capacity of Authorities: The adequacy of the law enforcement authorities' capacity to carry out their mandate, including their human and financial resources, their level of coordination, and the systems of information tracking at their disposal.

Scope of Money Laundering Offense

Compliance with international AML/CFT standards entails a thorough legal definition of the scope of a country's money laundering offense. Money laundering comprises a variety of activities, relating both to the predicate offenses that generated the "dirty" funds and to the transfer, concealment, possession and use of such funds. If a country does not adequately define money laundering, loopholes may exist that could enable or permit illegal money laundering activities.

Special care needs to be devoted to the issue of the mental state to be associated with the crime of money laundering. The criminal act of money laundering can encompass a variety of actors, having different levels of culpability and playing different roles in the money laundering process. If a country does not adequately address the mental state requirement, persons or legal entities who contribute to a money laundering offense may improperly escape criminal liability for their actions. To this end, countries must also permit mental state to be inferred from objective factual circumstances.

Finally, the scope of a country's money laundering offense ought to address the issue of legal person liability. If legal persons, such as corporations or associations, are not covered by a country's definition of a money laundering offense, these entities may be able to conduct money laundering activities without facing law enforcement authority sanctions – and thus serve as a "safe conduit" of laundered funds.

Principle 1: Definitional Scope of Criminal Offense of Money Laundering

Standard:

In accordance with FATF Recommendation 1²¹, we have used the 2000 United Nations Convention against Transnational Organized Crime (the “Palermo Convention”) and the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the “Vienna Convention”) for guidance in assessing Saudi Arabia’s compliance with this principle²². Specifically, in assessing the definitional scope of the criminal offense of money laundering, we have looked to the language in Articles 2 and 6 of the Palermo Convention, and Articles 1 and 3 of the Vienna Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be substantially in compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia’s compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia’s compliance with this principle.

Law:

In August 2003, Saudi Arabia enacted the Anti-Money Laundering Law (the “KSA-AMLL”)²³. The core definition of the criminal offense of money laundering is set forth in Article 2 of the KSA-AMLL, with certain aggravating circumstances singled out for more severe sanction in Article 17. Relevant terms are defined in Article 1.

We have found Saudi Arabia to be substantially in compliance with this principle from a legal perspective.

The definition of money laundering in Article 2 of the KSA-AMLL appears to be at least as broad as the corresponding language in the Palermo and Vienna Conventions. The aggravating circumstances in Article 17 of the KSA-AMLL closely track the language in Article 3(5) of the Vienna Convention.

The reason we do not consider Saudi Arabia fully compliant with this principle centers on the term definitions in Article 1 of the KSA-AMLL, which are not as rigorously drafted as the corresponding definitions in the Palermo and Vienna Conventions.

a. Proceeds.

The term “proceeds” as defined in KSA-AMLL Article 1(3) “shall mean any *funds* generated or earned directly or indirectly *from money-laundering offences* subject to sanctions hereunder” (emphasis added). In the Palermo Convention, Article 2(e) defines “proceeds of crime” as “any

²¹ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

²² The full text of both Conventions is appended to this report in Annex 1.

²³ The full text of the law is appended to this report in Annex 1.

property derived from or obtained, directly or indirectly, *through the commission of an offence.*” Therefore, (1) the Saudi definition excludes from the definition of “proceeds” any property derived from the commission of offenses other than money laundering offenses, and (2) the Saudi definition excludes any property other than funds.

a.1. *Property derived from non-money laundering offenses.*

The first exclusion does not effect a significant loophole because of the way the KSA-AMLL defines a money laundering offense. However, it does lead to unnecessary ambiguity regarding the relationship that prosecuting authorities would have to prove between the property in question and the offense to which it is connected.

Whereas the Palermo Convention instructs States Parties to criminalize “[t]he conversion or transfer of property, knowing that such property is the proceeds of crime,” the corresponding KSA-AMLL language is “[c]onducting any transaction involving property or proceeds with the knowledge that such property or proceeds came as a result of a criminal activity or from an illegal or illegitimate source.” This definition’s reference to “property or proceeds [derived from] an illegal . . . source” is somewhat awkward, in that the definition of the term “proceeds” appears to have already incorporated a connection to an illegal source. Nonetheless, the redundancy ensures that any property derived from any crime, including a non-money laundering crime, is covered by its provisions.

However, the Saudi language fails to clarify that the definition of a money laundering offense applies to transacting in property derived *directly or indirectly* from a non-money laundering crime. The definition of “proceeds” in Article 1 does spell out that proceeds can be earned or generated “directly or indirectly” from an offense – but it only covers money laundering offenses. The language in Article 2, regarding “property [that] came as a result of a criminal activity,” is useful in that it covers all crimes, but it does not make clear that “came as a result” includes indirect as well as direct derivation. Thus, it is arguable that for property derived from offenses other than money laundering offenses, the prosecuting authorities may have to prove that the property was derived *directly* from the crime – a higher burden than the one mandated by the Palermo Convention.

a.2. *Property other than funds.*

The second exclusion does not effect a significant loophole for reasons similar to those discussed above – the redundancy in the Article 2 language, which refers to both property and proceeds, allows the broad definition of “property,” which includes all types of assets, to supplement the narrower definition of “proceeds,” which excludes assets other than funds. However, this solution suffers from the same flaw – relying on the “property” language in Article 2 underscores the ambiguity regarding the requisite connection between “property” and the offense from which it is derived.

b. *Property.*

The term “property” as defined in KSA-AMLL Article 1(2) “shall mean any kind of assets and property, whether material or immaterial, movable or immovable, and legal documents and instruments which prove the ownership of the assets or any right attached thereto.” Article 2(d) of the Palermo Convention defines “property” as “assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.” It is unclear whether the reference to “right attached

thereto” in the KSA-AMLL corresponds to the Palermo Convention’s “interest in” the assets. It is arguable that the Saudi definition excludes documents and instruments evidencing an interest in assets.

Although we understand that Saudi property law does not recognize interests in property other than ownership²⁴, such an exclusion of interests in assets – e.g. leaseholds – from the definition of property would be improper. Money laundering is a transnational phenomenon, and the Saudi judiciary should be equipped to rule on cases involving interests in assets held in jurisdictions that recognize such interests, even if Saudi Arabia itself does not recognize them.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective. We have been informed by official sources that the Saudi Ministry of Justice is conducting training for *shari’a* judges on money-laundering offenses.²⁵ However, we have no details on the content of such training; therefore, we cannot assess whether such training sufficiently ensures that the definitional scope of the money laundering offense is understood and implemented by the judiciary.

²⁴ Interview with a Saudi attorney, 12/13/03. We understand that interests in property other than ownership are given de facto recognition in Saudi courts. However, this recognition has not been formalized *de jure* to our knowledge, thus leaving open the question of the treatment of such interests in the KSA-AMLL.

²⁵ Interview, Senior U.S. Government official, 11/21/03

Principle 2a: Mental State Requirement of Criminal Offense of Money Laundering

Standard:

In accordance with FATF Recommendation 2(a)²⁶, we have used the Palermo Convention and the Vienna Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the mental state requirement of the criminal offense of money laundering, we have looked to the language in Article 6 of the Palermo Convention, and Article 3 of the Vienna Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The core definition of the criminal offense of money laundering, set forth in Article 2 of the KSA-AMLL, describes the mental state required by the offense.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The mental element required by the KSA-AMLL definition of the criminal offense of money laundering is in line with the language of the Vienna and Palermo Conventions – namely, knowing that the property in question came as a result of criminal activity suffices to convict a defendant, even if such knowledge was not accompanied by an intent to assist the process of money laundering.

The reason we consider Saudi Arabia only partially compliant with this principle has to do with two main concerns.

First, Article 21 of the KSA-AMLL exempts from liability “those acting in good faith.” Since Article 2 already incorporates a mental state requirement into the definition of the offense, the need for the language in Article 21 is unclear. To the extent that an interpreter of the law, such as a judge, chooses to give Article 21 any effect – i.e., to acknowledge a “good faith” defense beyond the one inherent in the mental state requirement – the KSA-AMLL's language defining the mental state element of a money laundering offense would be undermined.²⁷

Second, we note that the KSA-AMLL makes no explicit provision for inferring mental state from objective factual circumstances. There is no language in it that corresponds to Article 6(2)(f) in the Palermo Convention, or Article 3(3) of the Vienna Convention. We also note that the treatment

²⁶ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

²⁷ According to a Saudi attorney, whom we interviewed on 12/13/03, the impact of the “good faith” exculpatory clause is unlikely to be significant.

of evidence in *shari'a* is heavily focused on confessions and witnesses, rather than circumstantial evidence.²⁸

Additionally, we note that the KSA-AMLL makes no reference to “willful blindness” or “conscious disregard” as being sufficient to satisfy the “knowledge” mental state requirement outlined in Article 2. The international standards we used in evaluating Saudi Arabia’s compliance with this principle do not require that the jurisdiction expressly establish “willful blindness” or “conscious disregard” as meeting the mental state requirement; nonetheless, failure to do so raises the possibility of a serious loophole in the criminalization regime.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective.

²⁸ According to a Saudi attorney, whom we interviewed on 12/13/03, there are few limitations on judicial notice in the *shari'a* court system. Thus, in practice, a judge could choose to infer mental state from circumstantial evidence – however, the admissibility of such an inference is not provided for by law and would depend on the judge’s personal amenability to this type of argument.

Principle 2b(1): Extension of Money Laundering Criminal Liability to Legal Persons

Standard:

We have used the Palermo Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the extension of liability to legal persons, we have looked to the language in Article 10 of the Palermo Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Articles 3-10 of the KSA-AMLL discuss "Financial and Non-Financial Institutions" ("Institutions") and their obligations and liabilities under the KSA-AMLL. Article 18 establishes penalties for natural persons who are members of Institutions and fail to comply with the obligations set forth in Articles 4-10 (mainly administrative obligations and reporting requirements). Article 19 establishes penalties for Institutions that violate Articles 2 and 3, which relate to the primary offenses of ML/FT.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The penalty imposed on Institutions that commit ML/FT offenses – which occurs when "such offenses [are] committed in their name or to their account" (Article 3) – is "a fine ranging from SR 100,000 [US \$26,667] up to the value of the property involved in the offence" (Article 19). This would appear to satisfy the FATF recommendation of effective, proportionate and dissuasive sanctions. Moreover, the administrative obligations in Articles 4-10, backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US \$133,333]" (Article 18), enhance law enforcement agencies' ability to discover and investigate offenses by legal persons. Such enhancement serves to increase the deterrent effect of the penalties for legal persons' violating the primary obligations of Articles 2-3.

The reason we consider Saudi Arabia only partially compliant with this principle is the limited reach of the defined term "Financial or Non-Financial Institution."

Article 1(5) of the KSA-AMLL defines the term as "any establishment in the kingdom engaged in any one or more financial, commercial or economic activity such as banks, money-exchangers, investment companies, insurance companies, commercial companies, establishments, professional firms or any other similar activities set forth in the Implementation Rules." This definition excludes legal entities that are not engaged in financial, commercial or economic

activities, such as charities, religious associations, educational institutions and other non-profit organizations.

Although Article 2 of the KSA-AMLL, criminalizing the core ML/FT conduct, applies by its terms to “anyone” – presumably including all legal entities – the terms of Article 19 suggest that legal entity-level penalties are only applied to Financial or Non-Financial Institutions. It is unclear whether the KSA-AMLL imposes any penalties at all on non-profit organizations at the legal entity level.

In light of the important role that such non-profit organizations play in a devout Moslem society, the failure to extend the KSA-AMLL’s reach to this class of legal persons constitutes a severe curtailment of the law’s effectiveness in combatting ML/FT offenses.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective. We have not been able to obtain data on enforcement of the KSA-AMLL’s money laundering provisions against any legal entities. We have not been able to obtain data on the extent or nature of criminal law enforcement agencies’ investigation and prosecution efforts against any legal entities.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective. We have not been able to ascertain whether all types of legal entities in Saudi Arabia – financial institutions, commercial institutions, social and non-profit institutions – regard themselves as being covered by the KSA-AMLL’s money laundering provisions.

Scope of Terrorist Financing Offense

Compliance with international AML/CFT standards entails a thorough legal definition of the scope of a country's terrorist financing offense. This requires an adequate definition of both the predicate offense of terrorism, and of the conduct that constitutes the financing thereof. If either of those are not sufficiently addressed by a country's criminal law regime, certain avenues of terrorist financing will remain legally available to offenders.

In addition, the same attention to mental state requirements and legal person liability is necessary in the terrorist financing context as in the money laundering context; failure to address these issues leads to analogous consequences.

Principle 42: Definitional Scope of Criminal Offense of Terrorist Financing

Standard:

We have used the UN CFT Convention and the UNSC R1373 for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be non-compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Saudi Arabia signed the UN CFT Convention in November 2001, and has not ratified it²⁹. UNSC R1373, adopted under Chapter VII of the UN Charter, is automatically mandatory on Saudi Arabia with no further action necessary on the kingdom's part. The offense of terrorist financing is set forth in the KSA-AMLL in Article 2(d).

We have found Saudi Arabia to be non-compliant with this principle from a legal perspective.

Article 2(d) of the KSA-AMLL provides that anyone who engages in “[f]inancing terrorism, terrorist acts and terrorist organizations” shall be deemed a perpetrator of a money laundering offense, subject to the sanctions associated with that offense.

We consider Saudi Arabia non-compliant with this principle for a number of reasons.

a. Definition of Terrorism.

We have not found any Saudi legislative definition of the crime of terrorism, despite its obligation under UNSC R1373, Article 2(e), to ensure that “terrorist acts are established as serious criminal offences in domestic laws and regulations”. We also note that Saudi Arabia is not a signatory to the UN CTB Convention³⁰, which provides an internationally accepted definition for terrorist bombings in its Article 2.

We are concerned over the possibility that Saudi Arabia's judicial construction of the definition of terrorism (as the predicate offense for terrorist financing) might exclude acts and organizations deemed terrorist in nature by international law. We note that the Arab Convention for the Suppression of Terrorism, and the Convention of the Organization of the Islamic Conference on Combating International Terrorism, to both of which Saudi Arabia is a signatory, define as a terrorist

²⁹ Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty11.asp> (last visited on Nov. 16, 2003).

³⁰ Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty9.asp> (last visited on Nov. 16, 2003).

crime and a terrorist offense, respectively, only acts of terrorism committed in the Contracting States or against their nationals, property or interests. Even should this definition be broadened by analogy to include acts committed against non-Contracting States, both treaties' definitions of terrorism exclude acts of armed struggle against foreign occupation. This exclusion would appear to cover, for example, acts by Chechen separatists against Russian civilians, acts by splinter IRA factions against British civilians, and acts by Palestinian rejectionist groups against Israeli civilians – all of which are recognized as terrorism by international law.

b. *Definition of Financing.*

The KSA-AMLL is insufficiently detailed with respect to its definition of terrorist financing. The UN CFT Convention, which is used as a benchmark by FATF, sets forth in Article 2(1) a more detailed and specific definition, including an intentional element (*mens rea*); its language reads, in relevant part,

Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out [acts of terrorism].

UNSC R1373, also used as a benchmark by FATF, provides the following specific language in Article 1 as guidance:

[A]ll States shall . . . [c]riminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts . . .

[and p]rohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.

We understand that laconic legal definitions are not uncommon in Saudi *nizams*, and that such definitions are later augmented by administrative regulations.³¹ However, we have not seen any such regulations on the subject of terrorist finance, and we are concerned over the vagueness of the KSA-AMLL itself.

The conditioning of the financial assistance to the family upon the “martyrdom” of the suicide bomber would appear to meet the UNSC R1373 definition of terrorist financing, as an indirect benefit to the terrorist that alleviates his or her concerns for his or her family’s financial security. However, it is doubtful whether such fund-collection would meet the KSA-AMLL definition of financing terrorism.³²

c. *Mental State Requirement.*

³¹ Interview with Professor Sherif Hassan of Columbia Law School.

³² According to a Saudi attorney, whom we interviewed on 12/13/03, the KSA-AMLL almost certainly does not cover financial assistance to the Palestinian’s armed struggle against Israel.

In contrast to the KSA-AMLL's definitions of money laundering offenses in Article 2(a)-(c), the definition of a terrorist finance offense in Article 2(d) does not specify a mental state requirement. Also, see analysis under Principle 2a.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 2b(2): Extension of Terrorist Financing Criminal Liability to Legal Persons

Standard:

We have used the Palermo Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the extension of liability to legal persons, we have looked to the language in Article 10 of the Palermo Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Articles 3-10 of the KSA-AMLL discuss "Financial and Non-Financial Institutions" ("Institutions") and their obligations and liabilities under the KSA-AMLL. Article 18 establishes penalties for natural persons who are members of Institutions and fail to comply with the obligations set forth in Articles 4-10 (mainly administrative obligations and reporting requirements). Article 19 establishes penalties for Institutions that violate Articles 2 and 3, which relate to the primary offenses of ML/FT.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective. See analysis under Principle 2b(1).

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have not been able to obtain data on enforcement of the KSA-AMLL's terrorist financing provisions against any legal entities. We have not been able to obtain data on the extent or nature of criminal law enforcement agencies' investigation and prosecution efforts against any legal entities.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have not been able to ascertain whether all types of legal entities in Saudi Arabia – financial institutions, commercial institutions, social and non-profit institutions – regard themselves as being covered by the KSA-AMLL's terrorist financing provisions.

Sanctions

Compliance with international AML/CFT standards as regards a country's criminal law regime requires that effective and dissuasive sanctions be available to punish those who engage in

money laundering or terrorist financing conduct. Failure to provide, enforce or implement such sanctions will undermine the efficacy of any criminalization of ML/FT. In addition, appropriate authorities must have the ability to attach assets of persons involved in ML/FT offenses, to prevent their being transferred beyond the reach of the jurisdiction's enforcement arms.

Special care must be given to the definition of the assets subject to attachment or confiscation. For example, if a country distinguishes between assets directly involved in money laundering or terrorist financing and assets not directly involved, confiscatory sanctions may lose their power and deterrent effect, due to the ease with which some types of assets can be converted into others.

Principle 17a: Effective Criminal Sanctions

Standard:

We have used FATF Recommendation 17³³ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Sanctions relevant to the AML/CFT criminal law in Saudi Arabia are provided in Articles 16-17 of the KSA-AMLL.

We have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Under the KSA-AMLL, a natural person found to be the perpetrator of a money laundering or terrorist financing offense is punishable by imprisonment of up to ten years and a fine of up to S.R. 5,000,000 (~ US \$1,333,333) (Article 16); this penalty is increased to 15 years and S.R. 7,000,000 if certain aggravating factors are present (Article 17). In addition, property, proceeds and instrumentalities connected with the crime are subject to confiscation. See also analysis of regulatory sanctions and legal entity sanctions, under Principle 17b.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have been unable to determine whether law enforcement and prosecutorial agencies are seeking to take full advantage of the punitive range provided by the KSA-AMLL's sanctions provisions.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have been unable to assess the range of penalties meted by the *shari'a* courts for ML/FT offenses, and the extent of any deterrence engendered by such penalties.

³³ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 3: Confiscating and Attaching Money Laundering-Related Assets

Standard:

In accordance with FATF Recommendation 3³⁴, we have used the Palermo Convention and the Vienna Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing provisional measures and authority for confiscation, we have looked to the language in Article 12 of the Palermo Convention, and Article 5 of the Vienna Convention.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with the confiscation portion of this principle, and we have found Saudi Arabia to be substantially compliant with the attachment portion of this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL establishes a procedure for attaching assets in Article 12, and authorizes confiscation of assets in Article 16.

We have not been able to verify Saudi Arabia's compliance with the confiscation portion of this principle from a legal perspective. We have found Saudi Arabia to be substantially compliant with the attachment portion of this principle from a legal perspective.

a. Confiscation.

Article 16 of the KSA-AMLL subjects the "perpetrator of a money-laundering offence under Article (2) [to] the confiscation of the property, proceeds and instrumentalities connected with the crime. If such property and proceeds are combined with property generated from legitimate sources, such property shall be subject to confiscation pro rata with the estimated value of the illegitimate proceeds." The provision for pro rata confiscation of intermingled assets corresponds to Article 12(4) of the Palermo Convention and Article 5(6)(b) of the Vienna Convention.

We do not consider the Article 16 grant of confiscatory authority to be sufficient evidence of compliance with this principle for the following reasons:

a.1. Conversion.

Article 12(3) of the Palermo Convention and Article 5(6)(a) of the Vienna Convention require States Parties to ensure that, if proceeds of crime are transformed or converted into other property, such other property shall be liable to confiscation instead of the proceeds. The KSA-AMLL contains no such provision. Due to the ease with which some types of assets can be

³⁴ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

converted into others, this omission in the KSA-AMLL could severely undermine the reach of its confiscatory sanctions, unless addressed elsewhere in the Saudi legal system through provisions we have not seen.

a.2. *Income and benefits.*

Article 12(5) of the Palermo Convention and Article 5(6)(c) of the Vienna Convention require States Parties to ensure that income or other benefits derived from proceeds of crime – or property into which proceeds of crime have been converted – is subject to confiscation. The KSA-AMLL contains no such provision.

a.3. *Alternative property.*

Article 12(1)(a) of the Palermo Convention and Article 5(1)(a) of the Vienna Convention require States Parties to adopt measures to enable confiscation of property “the value of which corresponds to” that of proceeds of crime. This enables the State Party to deal with situations in which the proceeds of crime are not amenable to confiscation, by confiscating instead other property of equal value. The KSA-AMLL contains no such provision. Indeed, we are given to understand that *shari’a* does not permit the confiscation of any property other than the specific property that was implicated in the wrongful act in question.³⁵

b. *Attachment.*

Article 12 of the KSA-AMLL authorizes the Financial Intelligence Unit (the “FIU”) to direct government authorities “to attach properties, proceeds and instrumentalities committed in money laundering for a period not exceeding 20 days. If further extension is needed, the order must come from the competent court.” This language provides the FIU with the necessary authority to cause assets to be frozen, and thus prevent them from being transferred or concealed, while proceedings meant to determine whether the assets should be confiscated take their course.

The reason we do not consider the Article 12 grant of attachment authority fully compliant with this principle is the brevity of the authorized attachment order. We are concerned that 20 days might not be sufficient for obtaining the requisite “order . . . from the competent court”, especially during Ramadan or in summertime, when the pace of judicial proceedings in Saudi Arabia slows measurably³⁶. Nonetheless, under most circumstances this period of time should be adequate, and therefore we consider the Article 12 language substantially compliant.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective.

³⁵ Interview with a Saudi attorney, 12/13/03.

³⁶ Interview with a Saudi attorney, 11/11/03.

Principle 43: Confiscating and Attaching Terrorist Assets

Standard:

In accordance with FATF Special Recommendation 3³⁷, we have used the UN CFT Convention and the UNSC R1373 for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be non-compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL's confiscation and attachment provisions, discussed under Principle 3, provide the authority for confiscating and attaching terrorist assets.

We have found Saudi Arabia to be non-compliant with this principle from a legal perspective. In addition to the issues outlined in Principle 3 regarding the efficacy of the KSA-AMLL confiscation and attachment provisions in general, the following additional concerns relate to those provisions as applied to terrorist finance offenses:

a. *Assets of terrorists and terrorist organizations.*

Article 1(c) of UNSC R1373 calls upon States to

[f]reeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities
...

The language quoted above clearly instructs States to freeze assets of terrorists and terrorist organizations, without limiting its reach solely to those assets that have actually been committed to the financing of terrorism. By contrast, the attachment provisions in Article 12 of the KSA-AMLL, and the confiscation provisions in Article 16, limit themselves to "properties, proceeds and instrumentalities" that are connected to the crime.

b. *Pro rata confiscation of intermingled funds.*

³⁷ The full text of the FATF 8 Special Recommendations on Terrorist Financing is appended to this report in Annex 2.

Article 16 of the KSA-AMLL states that if “property and proceeds [connected with the crime] are combined with property generated from legitimate sources, such property shall be subject to confiscation pro rata with the estimated value of the illegitimate proceeds.” The wording of this provision appears to place a considerable segment of terrorist financing assets beyond the reach of the KSA-AMLL’s confiscatory power.

“Proceeds” are defined in Article 1(3) as funds generated from money laundering offenses (including terrorist finance offenses). This definition does not cover assets that are intended for use in terrorist acts, if they are not originally derived from a criminal activity. Therefore, in the case of intermingled assets that include property intended for use in terrorist acts as well as other property, “the estimated value of the illegitimate proceeds” will be nil, and the pro rata confiscation will perform be limited to nil – as long as the terrorist financing assets themselves are not derived from a criminal activity.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective.

Designation of Authorities

Compliance with international AML/CFT standards requires appropriate formal designation and legal empowerment of law enforcement agencies. If a country does not designate such authorities to assume responsibility for AML/CFT enforcement, significant obstacles may exist with regards to the efficient monitoring of money laundering and terrorism financing, as well as to the appropriate reporting of these crimes. Lack of clarity in the designation can lead to confusion among law abiding citizens, such as employees of a financial institution or any other business, regarding their legal obligation to report a suspicious transaction or the appropriate method of reporting money laundering and terrorism financing offenses. Other obstacles may arise if several competing government organizations claim the right to enforce the law, as well as monitor, report and prosecute money laundering and terrorism financing offenses.

In addition to the problems inherent in a faulty formal designation of appropriate authorities, the designated authorities will face further problems and obstacles to enforcing the law unless they have the appropriate legal empowerment. In particular, they must have the authority to obtain pertinent documents and information from persons and institutions. Without such legal authority, enforcement agencies will be severely hampered in carrying out their mandate.

Principle 27: Designation of Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 27³⁸ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL designates authorities to enforce its criminal provisions and assist in AML-CFT investigations. Article 27 of the KSA-AMLL instructs the General Prosecution and Investigation Authority (GPIA) to investigate and prosecute ML/FT crimes. Article 11 of the KSA-AMLL establishes an FIU "to confront money laundering" and to serve as a clearing-house for all information relating to AML-CTF.

Although SAMA is not directly charged with criminal law enforcement, it is expected to play a role in the enforcement community. Its Charter grants it broad supervisory powers over the Saudi financial system. As the regulatory and supervisory authority over commercial banks, it is charged with preventing terrorists from exploiting the Saudi financial system and ensuring that banks follow AML-CTF regulations. The banking control department, under the direction of deputy governor of SAMA, is responsible for supervising banks' compliance with SAMA circulars and KSA laws and regulations. It is divided into sub-departments, such as the banking inspection department, the banking supervision department and the banking technology department.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The reason we consider Saudi Arabia only partially compliant with this principle is a lack of clarity regarding the role each of the designated authorities plays within the enforcement community, as well as the non-designation of authorities for a number of important functions specified in the KSA-AMLL.

a. Interaction with Ministry of Interior.

Although not specified in the laws to which we have had access, the police forces under the Ministry of the Interior also play a role in enforcement of the criminal sanctions provided for by the

³⁸ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex [X].

AML-CTF.³⁹ It is not clear to us how the Ministry of Interior is expected to interact with the above-mentioned enforcement authorities.

b. *Coordination.*

It is unclear whether these laws provide for an adequate level of coordination between the GPIA, the FIU, SAMA, and other enforcement agencies. It is important that coordination mechanisms be specified as part of the designation of authorities.

c. *Lack of Designations.*

In a number of instances, the KSA-AMLL establishes legal powers or obligations without designating the authority in which such power or obligation is to inhere. For example, Article 12 of the KSA-AMLL authorizes the FIU to “direct the concerned authorities to attach properties, proceeds and instrumentalities” upon “confirming” a suspicion of ML/FT conduct. Similarly, Article 15 instructs “the concerned authorities” to dispose of confiscated properties, proceeds and instrumentalities the destruction of which has not been ordered by the court.

We expect that these ambiguities will be resolved by the forthcoming Implementation Rules to the KSA-AMLL. Until such Rules are promulgated, however, the lack of designations for these ancillary powers and obligations will remain a potential impediment to the proper functioning of the law enforcement community as regards ML/FT offenses.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective. Our information does indicate, however, that members of the Saudi AML-CFT criminal law enforcement community are aware, to various degrees, of the new designations of authority.⁴⁰

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective.

³⁹ Interview, Senior U.S. Government official, 11/21/03

⁴⁰ Interview, Senior U.S. Government official, 11/21/03

Principle 28: Authority to Obtain Documents and Information

Standard:

We have used FATF Recommendation 28⁴¹ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's substantial compliance.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's full compliance in the banking sector.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's full compliance in the banking sector.

Law:

Article 8 of the KSA-AMLL requires Institutions to provide judicial and other concerned authorities with records and documents subject to applicable regulations. In the banking sector, Article 18 of the Banking Control Law (the "KSA-BCL") authorizes SAMA to conduct audits of any bank; Article 17 of the same law authorizes SAMA to require any bank to submit any statement according to SAMA forms.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's substantial compliance with the principle.

We have not been able to view the Saudi laws pertaining to general search and seizure authorizations, subpoena powers and the like. Although the laws cited above provide adequate authority to obtain documents and information from Institutions in the normal course of events, we note (1) that Institutions are defined to exclude non-profit organizations, and (2) that the laws cited above do not provide for search and seizure powers.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. Our limited information tends to indicate Saudi Arabia's full compliance with the principle in the banking sector.

According to Kevin Taecker, a former SAMBA official, SAMA installed an advanced inter-clearing banking system in 1998-99 to give it real-time access to transactions, in an effective utilization of its information-gathering authority.⁴² However, we have not been able to obtain

⁴¹ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁴² Interview with Kevin Taecker on 11/11/03.

systematic data on the use by law enforcement agencies of their authority to require documents and information, and we have not been able to obtain even anecdotal data on such use by law enforcement agencies outside the banking sector.

We have also been unable to obtain data on instances of non-compliance with requests for information, and any sanctions applied in such instances.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. Our limited information tends to indicate Saudi Arabia's full compliance with the principle in the banking sector.

We have anecdotal evidence suggesting that SAMA's authority to obtain documents and evidence has contributed to its effectiveness as a regulator. Taecker advised us that SAMA has excellent intelligence, and is highly aware of developments at Saudi banks. According to him, moreover, bank officials comply with any demand for information because SAMA is able to apply heavy sanctions.⁴³

⁴³ Interview with Kevin Taecker on 11/11/03.

Capacity of Authorities

Compliance with international AML/CFT standards entails ensuring the practical capacity of law enforcement agencies to carry out their functions. Most importantly, if designated authorities do not have sufficient human and material resources, their work may be seriously hampered, regardless of the legal authority afforded them. Such resources should be reflected in the form of adequate staffing levels, professional training specific to individual responsibilities, and adequate budget levels to fund requisite activities in countering money laundering and terrorist financing.

Absent adequate staffing levels, enforcement agencies may lack the manpower necessary to monitor and prosecute a significant volume of the money laundering and terrorist financing activities in the jurisdiction. Poor training of employees of the designated authorities may leave them unprepared to carry out the complex analysis necessary to unravel, understand and successfully prosecute sophisticated webs of money laundering and terrorist financing. Inadequacy in allocated budgets, meanwhile, may leave the designated authorities unable to acquire and utilize technological and other tools that can serve as “force multipliers” in both their monitoring and prosecution activities.

Another factor that could obstruct efficient and appropriate functioning of the designated authorities is a lack of coordination among themselves. A measure of the capacity of criminal law enforcement authorities, therefore, must include an assessment of the mechanisms that exists to ensure proper coordination within the enforcement community.

Finally, serious problems could also arise if the designated authorities do not have access to updated information tracking and statistics compiling systems. In light of the sophistication and creativity of prime actors in the money laundering and terrorist financing fields, law enforcement authorities without the institutional or technological ability to track information flow and analyze trends could be at a severe disadvantage in attempting to disrupt ML/FT activity.

Principle 30: Resources Available to Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 30⁴⁴ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

We have not been able to identify any appropriations bills or similar legislative actions outlining resources allocated to various agencies. We note that such legislative actions are not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

In order to adequately assess the capacity of Saudi Arabia's criminal enforcement institutions, we attempted to gather data on the budgets of the relevant institutions and divisions, the number of personnel dedicated to AML/CTF enforcement, and the level of training received by such personnel. Such data could be compared both to analogous figures from other countries and to data from previous years in Saudi Arabia, to provide a clear and sophisticated picture of Saudi efforts to counter ML/FT offenses.

We have found no information available on budget and staffing levels of any of Saudi Arabia's criminal enforcement agencies. We have uncovered anecdotal data on training practices. This anecdotal data confirms the Saudi government claim that it initiated a program to train judges and investigators in AML-CTF issues in February 2003.⁴⁵ We have no information on the content of

⁴⁴ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁴⁵ "Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism," Kingdom of Saudi Arabia, 2003. p. 6. Interview, Senior U.S. Government Official, 11/21/03

the training program or on how many people have been trained. From Congressional testimony, we have learned that the Mabahith are engaged in a joint CTF training effort with the FBI.⁴⁶ As of September, 2003, 20 Mabahith agents were being trained.⁴⁷ We have not been able to obtain information on the content of the program.

As an alternative measure of the resources allocated to Saudi criminal law enforcement authorities, we endeavoured to acquire data on the volume and quality of law enforcement activity to date in the AML/CTF field. Such data would include statistics on criminal trials for money laundering, sentences handed down for terrorist financing, assets seized, and so forth. Absent evidence of legal action by the enforcement authorities, even a record of the number of suspicious transaction reports filed by Saudi banks with SAMA could serve as an indirect measure of the resources devoted by the Saudi government to AML/CTF measures.

Again, we have found very little data available. The Saudi government has released figures claiming to have questioned over 2,000 individuals and arrested 250.⁴⁸ These actions were taken in the course of combating terrorism generally, not terrorist financing in particular. No statistics were available on the application of legal sanction to financial institutions for non-compliance with AML/CTF regulations. Former bankers in Saudi Arabia indicated, in our interviews with them, that they were only aware of legal action being taken in cases of fraud, and even those cases were rare.⁴⁹

An accounting of assets frozen is among the few points of solid data available. The Saudi government declared that, as of December 2002, it had investigated “many” accounts, and frozen 33 of them.⁵⁰ These accounts belonged to three different individuals and contained funds totaling \$5,574,196. Figures provided to the U.S. Senate in October 2003 put the Saudi freezes at 41 bank accounts belonging to 7 individuals for a total of \$5,697,400.⁵¹ This figure represents 4% of the total terrorist funds frozen worldwide since September 11, 2001.⁵² In the absence of more detailed information on the scope of law enforcement activity that led up to these asset freezes, it is difficult to base on them an estimate of the resources allocated to the enforcement agencies responsible for the freezes.

In short, outside of Saudi declarations, we do not have enough information to verify whether the Saudis have put in place adequate resources to conduct effective money laundering and terrorist financing investigations or launch prosecutions. Nor can we attempt to assess whether the resources allocated are adequate by reviewing Saudi results, as data on legal action is also lacking. Examples of unanswered questions include:

- how many people make up the FIU?
- what is the FIU’s budget?
- what are the qualifications of the staff making up the FIU and GPIA?

⁴⁶ John Pistole, testimony, House committee on financial services testimony on Sept. 24, 2003

⁴⁷ John Pistole, testimony, House committee on financial services testimony on Sept. 24, 2003

⁴⁸ “Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism,” Kingdom of Saudi Arabia, 2003. p. 4.

⁴⁹ Interviews with a Saudi banker and a former SAMBA officer.

⁵⁰ “Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism,” Kingdom of Saudi Arabia, 2003. p. 6.

⁵¹ Brisard, Jean-Charles. Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, October 22, 2003.

⁵² Brisard, Jean-Charles. Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, October 22, 2003.

- how many people in SAMA are devoted to combating terrorist financing?
- what is the status of the relevant training programs?
- what level of training is being offered?
- how many criminal trials for money laundering or terrorist financing have taken place?
- what percentage of STRs resulted in legal action?
- how many sentences were handed down?
- how severe were these sentences?

Principle 31: Coordination Among Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 31⁵³ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL establishes the FIU as a clearing-house for ML/FT information, but does not specify its role vis-à-vis other actors in the law enforcement community. Apart from the FIU, we have not found any legal basis for any coordinatory mechanism in the AML/CTF enforcement community. For instance, the KSA-AMLL designates the GPIA as the enforcement agency tasked with prosecuting money laundering and terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines, directed at banks, provide only oblique references to SAMA's cooperation with other agencies.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Apart from the FIU, we have not found any legal basis for any coordinatory mechanism in the AML/CTF enforcement community. For instance, the KSA-AMLL designates the GPIA as the enforcement agency tasked with prosecuting money laundering and terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines, directed at banks, provide only oblique references to SAMA's cooperation with other agencies. We note that such legislative basis for coordination is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁵³ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

We do not have information on cooperation among and between Saudi enforcement agencies or regulatory bodies in either the enforcement sphere or in developing new rules and regulations. Examples of types of data that would be helpful include data on the number of STR's filed or other information showing cooperation between supervisors, the FIU, compliance officers in financial institutions, and SAMA.

Principle 32: Information Tracking by Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 32⁵⁴ for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL directs the FIU to "be responsible for receiving and analyzing reports and prepare reports on suspicious operations from all Financial and Non-Financial Institutions."

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Apart from the oblique mention of "preparing reports" in Article 11 of the KSA-AMLL, we have not found any legal basis for any information tracking or statistic compiling mechanism in the AML/CTF enforcement community. We note that such legislative basis for information tracking is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Although the Saudis have cited the amount of terrorist assets frozen in various press releases, we have been unable to obtain any evidence that demonstrates that an orderly system for tracking this data exists. Furthermore, we are not aware of any money laundering or terrorist financing prosecutions having been made public. Thus, we are unable to evaluate if an effective record keeping system pertaining to this crime fighting data is being maintained.

⁵⁴ The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

We note, however, that SAMA has committed to implementing such a system: in Article 4.1 of the SAMA-AMLCTF, the agency states that it will “ensure that all banks are kept updated with the latest information on efforts to combat all economic crimes including anti-money laundering within Saudi Arabia and will distribute, on a half yearly basis, statistical information covering the total number of cases reported by region, currency, method, amount, lessons learnt, etc.” Should this commitment be fulfilled by SAMA, it would constitute a significant step toward the establishment of an information tracking system compliant with this principle.

Conclusions – Criminal Law

Our review and analysis of Saudi Arabia’s criminal law system as regards ML/FT offenses has highlighted a number of areas in which that system is fully or substantially compliant with relevant international standards. However, there are also several issues of concern, which will require continuing attention:

1. Saudi Arabia’s compliance with international standards on the definitional scope of the criminal offense of terrorist financing is unsatisfactory. Although Saudi Arabia has expressly outlawed the financing of terrorism, we have not been able to find a Saudi legal definition of the predicate offense of terrorism itself. Moreover, Saudi Arabia is not a signatory of the UN CTB Convention, which provides an internationally accepted definition for an important type of modern terrorism. The regional anti-terrorism conventions to which Saudi Arabia is a party contain definitions of terrorism that are inadequate in terms of both geographic reach (limited to the States Parties themselves) and scope of subject matter (excluding acts of “armed struggle against occupation”). This lack of clarity in Saudi Arabia’s legal definition of terrorism has the potential to undermine severely its prosecution of terrorist financing.

Another, related concern has to do with the vagueness of Saudi Arabia’s definition of financing. In contrast to the detailed language in relevant international instruments and conventions – including UNSC R1373 – outlining the definition of financing, Saudi Arabia has chosen not to define the term. This contrasts with Saudi Arabia’s commendable specificity in defining money laundering based on the language in relevant international instruments and conventions.

2. The lack of transparency regarding Saudi Arabia’s enforcement of its criminal laws relating to ML/FT is another main source of concern. This opaqueness prevented us from examining the human and material resources of the various enforcement agencies, as well as their ability to work with each other. In addition, it prevented us from analyzing the enforcement and prosecution activity to date in the AML/CTF field. By blocking both these lines of inquiry, the lack of transparency has left us – and, by implication, other open-source analysts, as well as the general public – unable to assess or verify the extent to which Saudi Arabia’s criminal law enforcement efforts are compliant with international standards, and indeed the seriousness of such efforts. Beyond the obvious undesirability of opaqueness on these important issues, we are concerned that this lack of publicly available information may undermine the deterrent effect of the Saudi AML/CTF criminal law regime.

3. A third major source of concern is the apparent exclusion of non-profit organizations, such as charities, from criminal liability as legal persons. We appreciate the fact that a charity’s officials are subject to criminal liability for ML/FT offenses as natural persons, and that such personal liability will doubtless impact the use of charities as ML/FT conduits. Nonetheless, it is important that the non-profit organizations themselves, as legal entities, be subject to criminal liability, especially in light of the important role that charities play in a devout Islamic society. Since such legal entity liability is extended to financial and commercial enterprises, we do not understand the failure to extend it equally to non-profit organizations.

Regulatory Regime

A vital component of a country's AML/CTF effort is its regulatory regime. This institutional structure creates a body of rules, regulations and requirements that delineate the responsibilities of financial, commercial, non-profit and informal entities. A regulatory regime also authorizes institutional oversight over these entities. Consistent implementation and enforcement by regulators creates a deterrent effect. In addition, the thoroughness with which a country monitors and sanctions ML/FT activity sends an important public message about its determination to eradicate such activity, while stigmatizing those who engage in it.

This chapter will examine six significant aspects of the regulatory regime component of Saudi Arabia's AML/CTF effort:

- Institutional measures to combat AML-CTF: Countries need to create an efficient institutional infrastructure in order to handle reporting, supervision, implementation and enforcement of the AML-CFT regulations by financial, commercial, non-profit and informal entities. In addition, appropriate administrative capacity and competent enforcement authorities are necessary to eliminate terrorist financing and identify, prosecute and sanction offenders.
- KYC requirements regarding customer identification and due diligence: Knowing the client is the cornerstone of an effective AML and CTF regime. Financial and non-financial institutions are vulnerable if they don't have a solid knowledge of their clients, the clients' source of funds, their business activities, and the control structure of the clients' entities. In addition, there are specific risks posed by special categories of clients, such as Politically Exposed Persons and Correspondent Banks.
- Monitoring and reporting transactions: The risk of money laundering and terrorist financing cannot be effectively reduced without ongoing monitoring of the transactions. If the institutions do not have the means to detect suspicious transactions, including systems (technology), adequate staff and knowledge, they could fail in their duty to report suspicious activity. The monitoring and reporting of transactions should be tailored for the level of risk of the account, implying a higher level of monitoring for high-risk accounts.
- Retention of Records: Records of transactions and identification data are necessary documents in order to reconstruct transactions and follow the money trail in an investigation. If such documents are destroyed, not maintained long enough, or are not made available to competent authorities, then the reconstruction of evidence is seriously impaired.
- Non-financial sector: Non financial institutions such as real estate businesses, law practices, precious metals and precious stone dealers are often used by criminals as conduits for laundering money or financing terrorism. Therefore, the same standards of regulation, supervision and due diligence must be applied to non financial institutions as they are applied to financial institutions.
- Non-profit sector (Charities): Non profit institutions play an important role in Saudi society. A variety of ministries and agencies have authority over the regulation of this sector. Delineations of authority are unclear. Given the recent history of abuse of charitable funds this sector requires analysis. Supervision and due diligence must be applied to non profit institutions as they are applied to financial institutions.

Institutional Measures to Combat AML-CTF

Financial and non-financial entities are subject to money laundering and terrorist financing risks resulting from inadequate controls and procedures. The country's secrecy laws as applied to financial institutions could interfere with the implementation of Anti-Money Laundering policies. This problem is especially relevant in cooperation with authorities and sharing information between institutions.

In addition to having the legal structure in place, a country needs to create an efficient institutional infrastructure in order to handle reporting, supervision, implementation and enforcement of the AML-CFT regulations by the financial institutions.

Without the appropriate administrative capacity, the competent enforcement authorities will lack the resources necessary to eliminate terrorist financing and identify, prosecute and sanction offenders.

Principle 33: Preemption of Financial Institution Secrecy Laws

Standard:

A country's secrecy law should not inhibit the implementation of the FATF Recommendations.⁵⁵

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an implementation and enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The Regulations on Anti Money Laundering in KSA – Anti Money Laundering Law (“KSA-AMLL”) mentions confidentiality provisions in Articles 8, 13, 22 and 25. Article 25 is a safe harbor for persons who violate confidentiality provisions by performing their reporting duties. SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing (“SAMA-AMLCTF”) mention the importance of confidentiality provisions throughout the document, but also include a safe harbor (Article 12.4.D and Article 13.2) for banks and bank employees that notify SAMA or the FIU (see also Standard 34).

The provisions in the KSA-AMLL are unsatisfactorily vague regarding the interplay between secrecy laws and reporting requirements. Article 8 of the KSA-AMLL instructs Institutions to provide information to judicial or other concerned authorities “as an exception to the confidentiality provisions,”⁵⁶ but subject to unspecified “applicable regulations.” Article 13, expanding on the Article 8 language, specifies that information “discovered”⁵⁷ by Institutions and relating to a violation of the KSA-AMLL “may be shared with the concerned authorities” to the extent necessary for investigation or judicial action. Article 25, as a safe harbor, exempts directors, manager, employees, owners and agents of Institutions from liability for violating confidentiality provisions in the course of performing their KSA-AMLL obligations, unless they are proven to have “acted in bad faith to hurt the involved person.”

The safe harbor in Article 25 is limited to carrying out the duties set forth in the KSA-AMLL. These duties include notifying the FIU of suspicious transactions (Article 7); consequently, the safe harbor appears to prevent bank secrecy laws from interfering with the initial notification of the FIU regarding suspicious transactions. The duties also include cooperating with other “concerned authorities” (Article 8, and Article 13 which appears to draw its authority from Article 8). However, since the duty of cooperation with other authorities is made contingent on following the vaguely specified “applicable regulations,” we cannot assess the degree to which the safe harbor provides meaningful protection, absent an analysis of these regulations.

As regards regulations applying to the financial sector, we analyzed SAMA-AMLCTF to determine the degree to which it limits the cooperation detailed in Article 8 of the KSA-AMLL. Our analysis suggests that any cooperation other than through SAMA is forbidden by SAMA-AMLCTF.

⁵⁵ FATF Recommendation 4. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁵⁶ [Translation by Prof. Hassan]

⁵⁷ [Translation by Prof. Hassan]

Article 3.11 of SAMA-AMLCTF states that “[b]anks, as directed by SAMA, should provide all relevant details and documents, as and when required. Under any circumstances, customer information should not be released to any party without SAMA’s approval.” This language clearly prohibits banks from sending customer information to other parties, such as law enforcement agencies, except through SAMA or with SAMA’s permission.

Based on our analysis of the KSA-AMLL and SAMA-AMLCTF, we are concerned that the Saudi regulatory framework appears to exempt only interactions with SAMA and the FIU from the strictures of the financial confidentiality provisions. Although we acknowledge the efficiency and professionalism of SAMA, the inhibition of communications between banks and other enforcement agencies places unnecessary strain on SAMA as a conduit of information.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

The “safe harbor” provision as described above has been recently enacted and its implementation could not be assessed. With regards to conflicts between the country’s financial institutions secrecy laws and the need to share information between institutions, Saudi Arabia’s strict secrecy laws are not an exception. Switzerland, for example, has very stringent secrecy laws as well, going as far as prohibiting the sharing of information between the local branch and the overseas headquarter. However, western financial institutions operating in Switzerland often require their clients to sign a waiver in which they give the institution holding their accounts permission to share information with the parent company abroad as needed⁵⁸. As far as we could determine, Saudi Arabia does not follow this practice.

⁵⁸ Interview with compliance officer at large international bank November 5, 2003.

Principle 34: Protection from Liability for Disclosure

Standard:

There must be legal provisions protecting financial institutions' officers from criminal and civil liability in order to ensure that suspicious activities are properly reported without the fear of personal liability for breaching client confidentiality. These provisions should cover financial institutions, their directors, officers and employees in terms of protection from criminal and civil liability for breach of any restriction on disclosure to the FIU, if the information was reported in good faith. This provision should apply even when the underlying criminal activity is not known, or whether an illegal activity actually occurred.⁵⁹

Assessment:

From a legal perspective, the Saudi law is fully compliant.

From an implementation and enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Protection of persons from liability for reporting suspicions to the authorities is covered in Article 25 of the KSA-AMLL, and in Articles 12.4.D and 13.2 of SAMA-AMLCTF.

The KSA-AMLL provides that owners, managers, employees and agents of Institutions "shall be relieved from criminal, civil or administrative liability that may be caused by performing the duties provided for herein or by violating the provisions of confidentiality, unless it is established that they acted in bad faith to hurt the involved person" (Article 25). Meanwhile, SAMA-AMLCTF, in the context of suspicious transaction reporting, states that "[t]he notifying bank and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith" (Article 12.4.D). SAMA-AMLCTF further states, in the context of its tipping prohibition, that "[n]otification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi Arabian Banking Laws and Regulations" (Article 13.2).

Implementation/Enforcement:

The implementation and enforcement of the safe harbor provision is discussed under Principle 1. However, according to FATF 14a, the safe harbor provision should apply to disclosure to the FIU. In Saudi Arabia the FIU is not fully operational yet. Financial Institutions are instructed to make all the disclosures to SAMA directly, or not make any disclosures at all to any other government institution without consulting SAMA and obtaining permission from SAMA to do so.⁶⁰

⁵⁹ FATF Recommendation 14a. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁶⁰ Interview with former senior SAMBA employee, November 12 2003

Principle 35: Prohibition on Tipping Off

Standard:

Financial Institutions should not disclose the fact that information about a client is reported to the FIU.⁶¹

Assessment:

From a legal perspective, the Saudi law is fully compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Prohibition on disclosing the fact that a suspicious transaction has been reported to the authorities is covered in Article 9 of the KSA-AMLL, and in Article 13.1 of SAMA-AMLCTF.

The KSA-AMLL requires that Institutions and their employees "shall not alert or permit to alert clients or other related parties about suspicions regarding their activities" (Article 9). SAMA-AMLCTF provides that "[b]anks shall not under any circumstances inform customers of their suspicion or of their notification to the authorities. Extreme caution must be exercised when dealing with these customers" (Article 13.1).

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁶¹ FATF Recommendation 14b. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 36: Development of Internal AML and CFT programs

Standard:

Financial Institutions should be mandated to develop internal AML and CTF programs that should include: internal policies, procedures and controls, employee screening procedures, ongoing training program, and an audit function to test the system.⁶²

Assessment:

From a legal perspective, the Saudi law is largely compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Both KSA-AMLL and SAMA-AMLCTF cover this principle. Article 10 of the KSA-AMLL applies both to financial and non-financial institutions.

Saudi programs against ML and TF include:

- i) Development of internal policies – This is covered by KSA AMLL, Article 10, a) and SAMA-AMLCTF 6.7. However, there is no provision for screening of employees. In Guidelines for Prevention of Money Laundering issued by SAMA in 1995 we found a provision regarding promoting Saudi nationals in positions sensitive to money laundering such as cashiers, tellers, etc, but no specific requirements with respect to screening of employees prior to hiring or on an ongoing basis.
- ii) Ongoing employee training program – This is covered by KSA-AMLL, Article 10, c) and SAMA-AMLCTF 5.2. Article 10 specifies that ongoing training programs should be developed for “specialized” employees, such that they would be able to identify and combat money laundering. This article does not cover all employees working for a financial or non-financial institution. Industry best practices recommend all employees should have ongoing training so that each employee is aware of and able to recognize and report suspicious activity. SAMA-AMLCTF 5.2 recommends training for all employees, but only front line and account opening personnel are subject to full training to be planned through the bank's annual compliance plan.
- iii) Audit function to test the system – This is covered by KSA-AMLL, Article 10, b) which only requires that the auditing function supervise the “availability of basic requirements to combat ML”. Compliant as per SAMA-AMLCTF 6.8.
- iv) External auditors as per Basel 59 – No provision was found in the KSA- AMLL or SAMA-AMLCTF, however this principle is covered in the SAMA Guidelines for Prevention of Money Laundering dated 1995.

Enforcement:

⁶² FATF Recommendation 15, Basel 18,19, 55-59. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

In interviews with former bank officers from KSA, we learned that the banks set up as joint ventures with a western bank are required to follow the internal policies of the western counterpart. According to these bank officers, these internal policies are very strict, in most cases exceeding the requirements of the national laws. We have not received the same degree of assurance regarding the purely Saudi banks.⁶³ We have not been able to assess compliance with this principle from an implementation and enforcement perspective by financial institutions other than banks or by the non-financial institutions.

⁶³Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.

Principle 37: Foreign Branches and Subsidiaries

Standard:

The standards employed by financial institutions in combating money laundering and terrorist financing should apply to branches and subsidiaries located abroad.⁶⁴

Assessment:

From a legal perspective the Saudi law is partially compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA-AMLL for foreign branches and subsidiaries.

SAMA-AMLCTF 5.4 recommends that standards followed by local financial institutions are also applied to branches and majority owned subsidiaries located abroad. From a legal perspective, SAMA is in compliance with the FATF requirements.

FATF further recommends that in cases in which local laws and regulations prohibit this implementation, the parent company should be notified. SAMA does not have a provision for this recommendation.

Furthermore, in 5.4 SAMA-AMLCTF specifies that "where local ML and TF legislation is in effect, this must be adhered to". The implication is that foreign branches and subsidiaries could have lower AML standards than the Saudi parent company, for as long as local legislation is adhered to. This implication could be also inferred from section 6.17.7 of SAMA-AMLCTF: "where a foreign branch, subsidiary or associate refers business to a bank in Saudi Arabia [...] the bank should [...] determine whether it complies with Saudi Arabian laws and regulations".

This contradicts Basel 66, which require that the higher standard of the two be applied in cases in which the standards of the two countries differ. In this respect, provision 5.4 of SAMA-AMLCTF is non-compliant.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁶⁴ FATF Recommendation 22, Basel 63-69. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 38: Effective Regulatory Sanctions

Standard:

Sanctions must be in place in order to strengthen the enforcement of the regulations, including criminal, civil and administrative, to be applied to legal and natural persons. The punishment for non-compliance with anti-money laundering or terrorist financing requirements must be clearly stated in order to achieve their purpose of deterrence and dissuasion.⁶⁵

Assessment:

From a legal perspective the Saudi law is fully compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Sanctions relevant to the AML/CFT regulatory regime in Saudi Arabia are provided in Articles 16-20 of the KSA-AMLL, and Articles 22 and 23 of the Banks Control Law (the "KSA-BCL").

Under the KSA-BCL, SAMA is authorized to sanction violations of its regulation by suspending or discharging any bank director or employee, suspending a bank's loan-granting and deposit-accepting authority, and revoking a bank's license (Article 22). In addition, individuals responsible for a violation may be sanctioned with a fine of up to S.R. 5,000 (US \$1,333) (Article 23(5)).

Under the KSA-AMLL, the penalty imposed on Institutions that commit ML/FT offenses – which occurs when "such offenses [are] committed in their name or to their account" (Article 3) – is "a fine ranging from SR 100,000 [US \$26,667] up to the value of the property involved in the offence" (Article 19). The administrative obligations in Articles 4-10 are backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US \$133,333]" (Article 18). Finally, Article 20, a type of basket provision, states that "[a]nyone violating a provision not stated hereof shall be subject to a jail penalty up to six months and a fine up to SR 100,000 [US \$26,667] or to either punishment." See also analysis of criminal sanctions on natural persons, under Principle 17a.

It is also noteworthy that, under Saudi *shari'a*, the concept of *ta'azir* ("discretionary penalty" offenses) permits a court to extend the reach of the sanctioning power beyond that set forth in the enacted law. With regard to *ta'azir* offenses that violate the public interest (*al-maslaha al-'amma*), *shari'a* principles allow an act that is otherwise permissible to be deemed an offense if the context renders such conduct harmful to public interest. This is an exception to the general rule that only conduct forbidden by textual authority can be sanctioned.⁶⁶

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have been unable to determine whether law enforcement and prosecutorial agencies

⁶⁵ FATF Recommendation 17. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁶⁶ Criminal Justice in Islam: Judicial Procedure in the Shari'a 71-72 (2003, Muhammad Abdel Haleem et al. ed.); Mohamed S. El-Awa, Punishment in Islamic Law: A Comparative Study 114-16 (1981).

are seeking to take full advantage of the punitive range provided by the KSA-AMLL's sanctions provisions for the administrative offenses specified in that law. Additionally, we have not been able to obtain any systematic data on SAMA's use of its sanctioning power under the KSA-BCL.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have been unable to assess the range of penalties meted out by the Shari'a courts for regulatory offenses under the KSA-AMLL, and the extent of any deterrence engendered by such penalties. However, anecdotal evidence does suggest that, within the financial sector, banking officials are highly aware of, and deterred by, SAMA's sanctioning power.

We have had inconsistent reports on whether the sanctioning power inducing such deterrent effect is indeed the sanctioning power granted to SAMA by law, or whether it derives from SAMA's [political] influence on other law enforcement agencies with different sanctioning powers.

Principle 39: Establishment of Guidelines for Creation of an AML Regime

Standard:

The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.⁶⁷

Assessment:

From a legal perspective the Saudi law is fully compliant.

From an implementation perspective the Saudi law is fully compliant with respect to financial institutions. We have not been able to verify Saudi Arabia's compliance with this principle with respect to non-financial institutions.

Law:

The Saudi Government has established guidelines for financial institutions and designated non-financial institutions to follow to create an effective AML-CTF regime. The KSA-AMLL, the SAMA-AMLCTF, and the Banking Control Law all set forth requirements for institutions to follow. The SAMA-AMLCTF regulations are especially relevant in this regard. In addition to mandating specific actions that institutions must take and establish parameters for such things suspicious transactions and know-your-customer policies, they provide recommended preventive procedures and offer an appendix on indicators of ML or TF activity.⁶⁸

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

The guidelines have been established.

We were unable to assess compliance from an implementation perspective with respect to assistance and feedback to financial and non-financial institutions by the competent authorities.

⁶⁷ FATF Recommendation 25. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁶⁸ Kingdom of Saudi Arabia, SAMA Banking Inspection Department, Rules Governing Anti-Money Laundering and Counter-Terrorist Financing, May 2003, 27-28 and 30-35.

Principle 40: Establishment of an FIU

Standard:

Countries should establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of Suspicious Transaction Reports (STRs) and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR⁶⁹.

The Egmont Group of Financial Intelligence Units also provides standards and statements of purpose for FIU's.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL establishes the Saudi FIU. However, the law states that "The Location of its [the FIU's] head office, its structure, its power and method of exercising its duties and connections" will be outlined in the implementation rules related to the AML laws. These rules were expected to be released by the end of November 2003, but to date, are still not available to us. The KSA-AMLL also designates the General Prosecution and Investigation Authority ("GPIA") as the enforcement agency tasked with prosecuting ML/FT offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies.

Article 4.1 of the SAMA-AMLCTF requires all local banks to report suspicious transactions to both the Saudi FIU and to SAMA.

We do not have enough data to assess Saudi Arabia's progress in this area. Most importantly, we do not have the implementation laws mentioned in Article 11.

In lieu of an evaluation, it is useful to briefly outline the major elements that we would expect to see in the new implementation rules as defined by the FATF methodology. Specifically, the new central body should meet the Egmont Group definition of an FIU as well as perform the mission outlined in the Statement of Purpose of the Egmont Group of FIU's.⁷⁰ Furthermore, the FIU should have the authority to request additional information from reporting parties, have access to financial, administrative and law enforcement information on a timely basis, be authorized to order sanctions against reporting institutions that fail to comply with their obligations, and be authorized to share information with both local and international law enforcement agencies.

⁶⁹ FATF Recommendation 26. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁷⁰ Statement of Purpose of the Egmont Group of Financial Intelligence Units, The Hague, June 13, 2001, http://www1.oecd.org/fatf/pdf/EGstat-200106_en.pdf (last visited on December 5, 2003)

It is important to note that some of the basic steps towards developing an FIU are already in the current laws. Specifically, the FATF methodology states that all financial institutions should be required to send any Suspicious Transaction Report (STR) to the FIU. Saudi institutions are already obligated to do this under Article 7 of the new Anti Money Laundering Laws. Furthermore, the FIU should issue guidelines for identifying complex transactions. Currently SAMA, the Saudi central bank, seems to be effectively fulfilling that role by issuing documents such as The Rules Governing Anti Money Laundering and Combating Terrorist Financing, which it released in May 2003.

Implementation/Enforcement:

The Saudi Government has recently created an FIU within the Ministry of Interior.⁷¹ We understand that this FIU is not yet fully functional, and that SAMA is currently fulfilling this role as a central clearinghouse for information on money laundering and terrorist financing.⁷² We have no data on resource allocations or implementation of the new AML laws and thus cannot assess Saudi compliance with this standard. Key missing pieces of information include: the power of the FIU to collect information from financial and non-financial institutions, the budget of the FIU, the number of staff allocated to the FIU as well as the level of staff training and the degree of coordination between other government authorities and the FIU.

⁷¹ Interview, Senior U.S. Government Official.

⁷² Interview, Senior U.S. Government Official.

Principle 41: Supervisory Authority

Standard:

Supervisors of the financial sector should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.⁷³

Assessment:

From a legal perspective, we have found Saudi Arabia to be substantially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 18 of the Banking Control Law (the "KSA-BCL") authorizes SAMA to conduct audits of any bank. Article 17 of the same law authorizes SAMA to require any bank to submit any statement according to SAMA forms.

Article 25 of the KSA-AMLL relieves owners, managers, representatives and employees of Financial and Non-Financial Institutions from liability for violating confidentiality provisions in the course of obeying the KSA-AMLL, unless they were acting in bad faith to hurt the involved person.

Sanctions:

Under the KSA-BCL, SAMA is authorized to sanction violations of its regulations by suspending or discharging any bank director or employee, suspending a bank's loan-granting and deposit-accepting authority, and revoking a bank's license (Article 22). In addition, individuals responsible for a violation may be sanctioned with a fine of up to S.R. 5,000 (~ US \$1,333) (Article 23(5)).

Under the KSA-AMLL, the administrative obligations in Articles 4-10 – which include reporting requirements and a duty to make certain documents available to supervisory authorities – are backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US \$133,333]" (Article 18).

Thus, SAMA appears to have the authority to compel banks to provide it with information as well as the power to sanction non-cooperation directly through the KSA-BCL, or indirectly by subjecting the non-cooperating entity to sanction under the KSA-AMLL.

Implementation/Enforcement:

Saudi law may vest the supervisory authorities with the necessary powers, but there is little indication that those authorities are exercising this power. We have yet to see, outside of occasional Saudi announcements about single incidents, concrete evidence of fund seizures, terrorist financing prosecutions, or sanctions placed on any Saudi banks for violating the new AML laws. Nor do we

⁷³ FATF Recommendation 29. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

have information on how often the Saudi government requests assistance from financial institutions for AML-CTF, and how often those requests are satisfied. Accordingly, we are unable to verify Saudi Arabia's compliance with this principle from the enforcement and implementation perspectives.

Principle 42: Resources Available to Regulatory Supervisors

Standard:

Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.⁷⁴

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Saudi Laws and Regulations do not set standards for financial, human or technical resources for government authorities. Article 10 of the KSA-AMLL instructs the relevant financial and non-financial institutions to employ qualified personnel to implement programs to combat money laundering and to provide specialized employees with continuing training about new ways and new technologies to fight money laundering and terrorist financing; however, no mention is made of the human resources available to the supervisory authorities. We note that such legislative specifications are not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

The financial and human resources discussed in this principle are key measures of Saudi Arabia's progress in combating terrorist financing. In order to adequately assess the capacity of Saudi Arabia's regulatory institutions, it is vital to know what the budgets of the relevant institutions and divisions are, how many personnel are working on AML/CTF issues, and what level of training they have received. Such information could then be compared to data from past years, to measure changes that might reflect a new awareness of the problem of terrorist financing; it could also be compared against benchmarks established by other countries.

Unfortunately, no information is available on budget and staffing levels of any of Saudi Arabia's regulatory authorities. A small bit of information is available on training practices. SAMA runs the Institute for Banking, which is the recognized qualifications and accreditation body for

⁷⁴ FATF Recommendation 30. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

professional practitioners in the banking and financial services sector in the Kingdom of Saudi Arabia.⁷⁵ It offers at least one course on Money Laundering issues to banking professionals. Further information on the activities of the institute in regard to AML-CTF is unavailable, as is any information on the training that SAMA employees themselves receive.

Though information on the capabilities of Saudi Arabia's regulatory authorities is lacking, some evidence of enforcement results would indicate that the institutions in question have the resources to fulfill their mandates. Unfortunately, hard data is unavailable in this area. Among the pieces of information that would be useful:

- Data on the number of audits that SAMA conducts and on the number of requests for information that it submits to banks.
- Data on sanctions that SAMA has leveled against banks and other institutions under its authority for failing to comply with the requirements placed upon them by AML/CTF laws and regulations. Sanctions could include fines, the dismissal of bank officials, or limits placed on a bank's future operations, up to and including the suspension of its license.
- Evidence, independent of SAMA, that the banks and other institutions are implementing the new requirements. Such compliance could be used to infer SAMA effectiveness. Such requirements include: filing suspicious transaction reports; establishing a Money Laundering Compliance Unit; retaining records for the appropriate period; establishing sound 'know-your-customer' practices. It must be noted, however, that number of STRs is not a good measure of progress on AML/CTF. It is impossible to say if a decrease in STRs over time means that there is less suspicious activity or that more of it is going undetected.

Though solid information is lacking, some anecdotal evidence casts a positive light on SAMA's general level of regulatory capability. Interviews with former employees at the Saudi-American Bank (SAMBA) and with Americans with significant experience in Gulf banking indicate that SAMA is held in high regard in the Saudi financial services community. Its personnel are thought to be professional, competent, and dedicated. Such evidence, however, lacks the comfort that would be provided by more substantial measures of capability.

⁷⁵ The Institute of Banking Website <<http://www.iob.com.sa/index.php?id=10&on=10>>

Principle 43: Cooperation Among Regulatory Bodies

Standard:

Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place to enable them to co-operate, and where appropriate, co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.⁷⁶

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The KSA-AMLL establishes the Saudi FIU, but defers definition of its powers and functions to the Implementation Rules, which we have not been able to obtain. Article 28 of the KSA-AMLL states that the Minister of Interior should cooperate with the Minister of the Economy and the Minister of Finance in creating the Implementation Rules for the KSA-AMLL. The KSA-AMLL also designates the General Prosecution and Investigation Authority ("GPIA") as the enforcement agency tasked with prosecuting money laundering, terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines are directed at banks, and provide only oblique references to SAMA's cooperation with other agencies. We note that such legislative basis for coordination is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

According to an interview with a senior compliance officer, SAMA does take international best standards into account when developing its rules and regulations.⁷⁷ However, we do not have information on cooperation among and between Saudi enforcement agencies or regulatory bodies in either the enforcement sphere or in developing new rules and regulations. For example, we have not

⁷⁶ FATF Recommendation 31. [The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁷⁷ Interview with a former bank officer from KSA, November 2003

been able to obtain data on the number of STR's filed or other data showing cooperation between supervisors, the FIU, compliance officers in financial institutions, and SAMA – data that would have been helpful in assessing compliance.

Finally, it is unclear to us how SAMA coordinates with the FIU regarding Suspicious Transaction Reports, which both agencies may receive.

Principle 44: Collecting and Maintaining Statistics

Standard:

Countries should ensure that their competent authorities could review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated and on money laundering and terrorist financing investigations.⁷⁸

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

An effective information tracking system is an important part of the FIU. Tracking the number of STRs by specific banks allows an FIU to examine if there are any banks under its jurisdiction that are underreporting suspicious transactions. Furthermore, authorities can also compare the number of AML/CFT investigations launched as well as the number of STRs filed to similar statistics in other countries. By doing so they can measure the effectiveness of the system that is in place and see if their results demonstrate an appropriate level of reporting and investigation, vis-à-vis the requirements of international standards.

Article 11 of the new AML laws stipulates the creation of an FIU⁷⁹. The specification of the exact nature, powers, and obligations of the FIU is deferred to the Implementation Rules, which we have not been able to obtain. Per Article 11, the FIU will be in charge of receiving and analyzing suspicious transaction reports⁸⁰. Article 4.1 of the SAMA Rules Governing AML-CTF states that a copy of these reports will be forwarded to SAMA.⁸¹ SAMA will keep statistical information on the total number of cases by region, currency, method, amount, and lessons learned. It will distribute this information to banks on a semi-annual basis⁸².

Although the lack of rules regarding the FIU's operation is a concern, it is likely that the FIU's information tracking requirements will be fully outlined in the implementation rules document, associated with the new AML laws. Once the rules are published it will be important to evaluate the record keeping requirements of the FIU.

Also, we note that legislative basis for information tracking is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

⁷⁸ FATF Recommendation 32. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

⁷⁹ Kingdom of Saudi Arabia, Regulations on Anti Money Laundering in KSA, Anti Money Laundering Law, August 2003, 4.

⁸⁰ Ibid 4

⁸¹ Kingdom of Saudi Arabia, SAMA Banking Inspection Department, Rules Governing Anti-Money Laundering and Counter-Terrorist Financing, May 2003, 11.

⁸² Ibid 11.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information indicates that Saudi Arabia is partially compliant with this principle, due to the role played by SAMA.

In the absence of an operational FIU, SAMA has taken on many of the roles that will eventually be transferred to the FIU. However, we have not been able to obtain any documents that demonstrate that SAMA or any other organization has been keeping track of these types of statistics.

KYC Requirements Regarding Customer Identification and Due Diligence

Knowing the client is the cornerstone of an effective AML and CTF regime. Financial and non-financial institutions could be exposed to abuses by money launderers if they don't have a solid knowledge of their clients, the clients' source of wealth and source of funds, their business activities to determine what are the normal patterns of transaction, and the control structure of the clients' entities. In addition, there are specific risks posed by special categories of clients, such as Politically Exposed Persons and Correspondent Banks.

The status of political persons allows them to take advantage of their power in either obtaining proceeds of corrupt activities or circumvent the regulatory system. Such persons are individuals who either hold or held prominent public functions, including heads of state and government, politicians and political party officials, senior government, judicial or military officials, senior executives of public corporations.

To prevent the misuse of financial and non-financial institutions by Politically Exposed Persons ("PEP"), countries should require these institutions to perform enhanced due diligence on their PEP clients.

Correspondent Banking is a relationship that enables banks to conduct business in jurisdictions in which they have no presence by using local banks in order to offer their clients products and services otherwise not offered directly. This arrangement opens the corresponding bank to money laundering risks resulting from insufficient knowledge about the clients of the respondent bank. Correspondent Banking has been identified by FATF as being one of the areas of concern with respect to money laundering.

Principle 45: Customer Due Diligence

Standard:

Financial and non financial institutions should undertake customer due diligence measures including identifying and verifying the identity of the customers, obtaining information about the intended nature of the business relationship, and creating a transaction profile for the customer. When identity could not be verified, the accounts should not be opened or the relationship should be closed⁸³.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

KSA-AMLL covers the Identification requirements in Article 4, applying to both financial and non financial institutions. The law prohibits carrying out transactions under anonymous or fictitious names. The identity of the client must be verified, however the law permits the verification of the ID upon concluding the commercial transaction, contrary to the FATF Recommendation #5, which allows the timing of verification at the end of the transaction only in limited number of circumstances, such as non face-to-face business, securities transactions and life insurance business.

SAMA- AMLCTF Article 5.1 covers mandatory policies regarding customer ID, customer due diligence, and closing of the accounts in cases in which identity could not be verified. Articles 6.1 and 6.3 deal in detail with the requirement for creating a customer profile in order to determine unusual patterns of transactions for reporting purposes. These articles cover both individuals and commercial relationships.

We were unable to obtain additional ID verification rules, which are stipulated in the Implementation Rules.

Additionally, we are missing important guides for ID verification issued by SAMA to financial institutions, which are referred to in the SAMA-AMLCTF.

⁸³ FATF 5 and Basel 22, 23. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Articles 6.10 and 6.11 mandate Know Your Customer Standards and policy implementations. Article 6.11 makes reference to “Rules Governing the Opening of Bank Accounts in Saudi Arabia and General Operational Guidelines” issued by SAMA in 2002. We were unable to obtain this document in order to assess the details of compliance of this principle with the International Standards.

Article 6.13 covers due diligence for Private Banking Customers and Article 6.14 covers minimum standards for personal accounts. Both articles make reference to SAMA circulars that were not available to us, therefore a complete assessment of compliance could not be performed.

Enforcement:

We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia’s compliance with this principle from an implementation perspective. "However, we do have concerns that Saudi culture, which emphasizes privacy, may be a hindrance to the effective implementation of KYC standards, which require institutional intrusion into the private finances. For example, ascertaining the source of an individual’s wealth is contrary to cultural norms under which people generally do not speak about a person’s wealth or property. Such determinations are further complicated by the fact that Saudi Arabia has no income tax system and little to no central accounting for the wealth and property in the Kingdom."

Principle 46: Politically Exposed Persons

Standard:

Financial institutions should perform extra steps in addition to the normal due diligence measures with respect to Politically Exposed Persons:

- a) have appropriate risk management system to determine whether the client is a PEP
- b) obtain senior management approval for establishing a business relationship with such clients
- c) assess the client's source of wealth and the source of funds
- d) conduct enhanced monitoring of the business relationship.⁸⁴

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA-AMLL, governing all financial and non-financial institutions, that addresses PEPs. The SAMA-AMLCTF, which governs the conducts of banks and related financial institutions, addresses PEPs in 5.1.6, 6.12.

We have found Saudi Arabia to be only partially compliant with this principle for the following reasons:

- a. *Lack of coverage of the House of Saud.*

Our analysis indicates a serious deficiency in the definition of a PEP in the SAMA rules. According to SAMA, a PEP is "any individual who occupies, recently occupied, is actively seeking, or is being considered of a *senior civil position* in a government of a country, state, or municipality or any department including the military, agency, (government owned corporations, etc)".⁸⁵ [emphasis added]

By contrast, Principle 41 of the Basel CP, which we used as an international standard in assessing Saudi compliance, defines PEPs as "individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials".

The SAMA definition, by limiting its scope to "senior civil positions," does not expressly cover the House of Saud as PEPs; under the Basel CP, members of the House of Saud would be covered as either having "prominent public functions" or having the equivalent, in an absolutist monarchy, of "political" (as contrasted with "civil") positions.

⁸⁴ FATF Recommendation 6 and Basel 41-44. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

⁸⁵ SAMA Rules Governing Anti Money Laundering and Combating Terrorist Financing, May 2003, 6.12.

b. *Lack of point-by-point compliance with applicable standards.*

In addition to the measures recommended by FATF, Principle 44 of the Basel CP recommends checking publicly available information to establish a client's PEP status. Principles 41-43 discuss the risk associated with PEP and suggest criminalization of corruption of civil servant and public officers in accordance with OECD Convention on *Combating Bribery on Foreign Public Officials in International Business Transactions*, adopted by the Negotiating Conference on 21 November 1997. In certain jurisdictions foreign corruption becomes a predicate offence for money laundering, therefore all AML laws and regulations apply (reporting suspicious transactions, internal freeze of funds, etc.).

A point-by-point comparison of SAMA's rules with these standards resulted in the following assessment:

- Identification of the PEP – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.1.
- Obtaining senior management approval for establishing a banking relationship with a PEP – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.1.
- Establishing the source of wealth and source of funds for a PEP – Saudi Arabia is non-compliant; we have not found a provision addressing this issue.
- Enhanced ongoing monitoring – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.2.
- Refusal to maintain a business relationship when there is reason to suspect corruption or misuse of public assets – Saudi Arabia is partially compliant; SAMA-AMLCTF 5.1.6 only requires the reviewing and reporting of suspicious transactions arising from known public corruption, not suspected public corruption.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Although the international standards and the industry best practices require enhanced due diligence for PEPs, we did not find evidence sufficient to confirm that the financial sector in Saudi

Arabia is adhering to these practices, in particular with respect to the royal family. When asked about the due diligence performed on PEPs, one bank officer responded that it is a known fact that their wealth was derived from oil, therefore no additional investigation of the source of wealth or the source of funds is performed.⁸⁶ A Saudi attorney suggested that a bank might find it difficult to refuse illicit requests from a PEP if that PEP is a director of the bank.⁸⁷

⁸⁶ Interview with a bank official, November 2003

⁸⁷ Interview with a Saudi attorney, 11/11/03.

Principle 47: Correspondent Banking

Standard:

Financial institutions should implement enhanced due diligence measures when conducting business with correspondent banks.

In addition, banks should refuse to enter into a relationship or stop dealing with banks from jurisdictions with poor KYC standards, inadequate supervision, or inadequate regulations for the financial institutions. This provision includes shell banks.

In accordance with FATF Recommendations 7 and 18⁸⁸, we have used Principles 49-52 of the Basel CP for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 6.19 of SAMA-AMLCTF covers provisions dealing with correspondent banking and prohibiting dealing with shell banks.

We do not consider the SAMA-AMLCTF's language to be fully compliant with this principle, based on the following analysis:

- Gathering information about the correspondent bank – Saudi Arabia is partially compliant, based on SAMA-AMLCTF 6.19. The language in 6.19 requires that financial institutions fully understand and document the respondent bank's management and nature of business. 6.19.5 specifies information required: location and nature of business. However, both the FATF and Basel documents suggest that additional due diligence is needed, including obtaining information about the correspondent bank's reputation, quality of supervision, whether the bank has been subject to a ML/FT investigation, its major business activities, and the purpose of the account.
- Assessing the correspondent bank's ML/FT controls – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.19.4 and 6.19.5 B, C, D, E.
- Obtaining senior management approval before establishing relationship – Saudi Arabia is not compliant; we did not find a provision addressing this point.
- Documenting the responsibilities of each institution in a corresponding banking relationship – Saudi Arabia is not compliant; we did not find a provision addressing this point.

⁸⁸ FATF Recommendations 7 and 18, Basel 49-52. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

- Verifying the identity and ongoing due diligence on third parties using the correspondent bank – Saudi Arabia is not compliant; we did not find a provision addressing this point.
- Refusal to enter into or continue a corresponding banking relationship with shell banks – Saudi Arabia is not compliant; we did not find a provision addressing this point.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 48: Non-Face-to-Face Customers

Standard:

Financial institutions should have policies in place to deal with non-face-to-face customers. The same standard of customer identification should apply to these customers as it applies to those met in person. Measures should be taken to mitigate the higher risk resulting from accepting non-face-to-face customers⁸⁹.

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 5.1.7 of the SAMA-AMLCTF mandates that no accounts should be opened for non-face-to-face customers. Regarding this principle SAMA goes above and beyond the FATF Recommendations and the industry practice. Accordingly, we have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁸⁹ FATF Recommendation 8 and Basel 45-48. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 49: Introduced Business

Standard:

Financial institutions accepting introduced business may rely on third parties for certain elements of the due diligence process, but the ultimate responsibility for knowing the customer rests with the financial institution. Financial institutions should make sure that the third party referring the business is regulated and supervised according to the FATF Recommendations⁹⁰.

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 6.17 of the SAMA-AMLCTF adequately addresses the issues raised by the acceptance of introduced business by third parties, in accordance with applicable international standards. Accordingly, we have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁹⁰ FATF Recommendation 9 and Basel 35-36. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 50: Special Purpose Legal Vehicles and Trusts

Standard:

Countries should take measures to prevent the use of legal persons and arrangements by money launderers. Information must be obtained and be made available to authorities about beneficial ownership and control persons of such legal entities⁹¹.

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 5.1.2 of the SAMA-AMLCTF addresses the issues covered under this principle. However, we do not consider its language to be adequately compliant with this principle, based on the analysis below.

Both FATF and the Basel CP recommend adequate, accurate and timely information on ownership and control of trust, nominee, fiduciary accounts and corporate vehicles that could be used as fronts (PICs, IBCs). As such, identification and KYC is required on the following:

- beneficial owners
- individuals with control of legal persons
- settlors/grantors
- beneficiaries
- trustees
- intermediate layers of ownership
- holders of bearer shares

SAMA 5.1.2, by contrast, provides only for KYC process on the beneficial owners, Power of Attorney holders and Trustees. There is no specific coverage of fiduciary accounts, bearer share companies, and corporate vehicles used for personal asset holding purposes.

Most significantly, there is no requirement for KYC process on the settlor/grantor of a trust, although this individual is the source of the funds.

⁹¹ FATF Recommendation 33 and 34 and Basel 31-34. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Monitoring and Reporting Transactions

The risk of money laundering and terrorist financing cannot be effectively reduced without ongoing monitoring of the transactions. Financial and non-financial institutions expose themselves to money laundering risks if they do not have an understanding of their clients' normal and reasonable patterns of transactions consistent with the business activities. If the institutions do not have the means to detect suspicious transactions, including systems (technology), adequate staff and knowledge, it will be extremely difficult to track terrorist funds. The monitoring and reporting of transactions should be tailored for the level of risk of the account, implying a higher level of monitoring for high-risk accounts.

Principle 51: Requirement to Report Suspicious Transactions (including Terrorist Financing)

Standard:

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations, or represent proceeds from criminal activity, they should be required to report promptly their suspicions to the competent authorities.⁹²

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Both the KSA-AMLL and SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing ("SAMA-AMLCFT") adequately provide for this sort of reporting, and consequently we have found compliant with this principle.

Article 7 of the KSA-AMLL requires that all financial and non-financial institutions immediately inform the FIU of suspicious transactions, and prepare a detailed report on the transaction and the parties involved.

Article 25 of the KSA-AMLL relieves owners, managers, representatives and employees of Financial and Non-Financial Institutions from liability for violating confidentiality provisions in the course of obeying the KSA-AMLL, unless they were acting in bad faith to hurt the involved person.

The SAMA-AMLCFT:

- instructs banks to report any reasonable suspicion to the authorities (Article 3.9),
- confirms their obligation to provide relevant details and documents to SAMA (Article 3.11),
- requires all local banks to report suspicious transactions to both the Saudi FIU and to SAMA (Article 4.1),
- directs banks to establish procedures for cooperating with enforcement authorities through an internal Money Laundering Compliance Unit, or MLCU (Article 7),
- charges banks with formulating suspicious transaction reporting (STR) procedures to ensure that employees report suspicious transactions to the MLCU (Article 12), and
- provides that notification of suspected ML/FT cases to the authorities does not conflict with bank secrecy and customer confidentiality regulations (Article 13.2).

Enforcement:

⁹² FATF Recommendation 13 and FATF Special Recommendation IV. The full text of the FATF 40 Recommendations on Money Laundering and FATF Special Recommendations on Terrorist Financing are appended to this report in Annex 1 and 2.

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have no evidence that Saudi Arabia has punished banks or other institutions for not reporting suspicious transactions.

Implementation:

It is difficult to tell whether or not the measures allowed for in these laws have been implemented in Saudi Arabia. The FIU to which financial institutions should report has only recently come on line (see Recommendation 26 for further detail).⁹³ We understand that in the absence of the FIU, SAMA has adopted its responsibilities in this regard, but information on SAMA's activities is lacking. We have been unable to obtain statistics on how many suspicious transaction reports (STRs) are ever filed with SAMA, the nascent FIU, or any other regulatory authority, or on if or how these authorities act on the STRs.

⁹³ Interview, Senior US Government Official, November 2003.

Principle 52: Monitoring of Unusual Transactions

Standard:

Financial institutions should have intensified monitoring of all complex, large, or unusual transactions that have no apparent economic reason or lawful purpose. An examination of such transactions should be conducted and the findings should be available to authorities. There should be intense monitoring of high-risk accounts.⁹⁴

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA AML Law regulating both financial and non-financial institutions. This is an area of concern, since the AML Law does not require non-financial institutions to monitor unusual transactions. Although financial institutions are covered by SAMA, we could not obtain specific laws and regulations dealing with non-financial institutions.

SAMA Rules Governing AML, 6.2.3 mandates the monitoring of complex, large or unusual transactions. The background and purpose of each transaction should be examined and exceptions should be reported.

Another area of concern is the transaction monitoring threshold. FATF recommends a threshold of USD/EUR 15,000 as the designated threshold for financial transactions carried out in a single operation or in several operations that appear to be linked. SAMA 6.2.1 mandates a much higher threshold for monitoring transactions at SAR 100,000 (USD 26,660) regardless of the level of risk assigned to the account.

SAMA 6.5.2 indicates that a high-risk account should be subject to close monitoring, but it does not specify what close monitoring entails.

Enforcement:

We have no information on the enforcement of this principle.

Implementation:

The implementation this principle has not been determined. Each bank has developed its internal policies, which are safeguarded as proprietary information. There is no public information available regarding the monitoring of transactions by financial institutions.

⁹⁴ FATF Recommendation 11 and Basel 53, 54. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

The monitoring of transactions is not mandated for non-financial institutions in the laws that were available to us. There is no information available regarding such activity.

"However, as with customer due diligence, we have concerns that a cultural emphasis on privacy may hinder the effective monitoring of individuals' personal wealth transactions."

Principle 53: Transactions with Countries which Insufficiently Apply the FATF Recommendations.

Standard:

Financial Institutions should give special attention to transactions with persons, companies and other financial institutions from countries which insufficiently apply the FATF Recommendations.⁹⁵

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

FATF recommends that in dealing with persons, including companies and financial institutions, from countries with insufficient application of FATF Recommendations, the financial institutions should:

- a) examine the background and purpose of the transactions
- b) establish the findings in writing
- c) be available to help competent authorities

In addition, countries are required to take appropriate countermeasures if such a non-compliant country continues to insufficiently apply the FATF Recommendations.

SAMA leaves each financial institution to develop its own internal policies to recognize and report suspicious transactions. No specific guidance is given in dealing with these transactions as per sections 12.1 and 12.2 of the SAMA-AMLCFT. Section 11.3, however, recommends extra due diligence for funds transferred from or to NCCT as defined by FATF. Section 6.5.3 recommends rating the customers who have dealings with the NCCTs as High Risk customers. We thus find Saudi Arabia compliant with this principle.

It must be noted, however, that the NCCT list is not comprehensive, as FATF has not yet completed the assessment of all countries. In addition, FATF only assesses the legal and regulatory compliance, not the implementation and enforcement of the regulations.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

⁹⁵ FATF Recommendation 21. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 54: Monitoring Currency Transactions

Standard:

Countries should consider:

- a. Implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.
- b. The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.⁹⁶

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 14 of the KSA-AMLL states that the Implementation Rules will define the regulations and procedures for the amount of cash and precious metals that can be carried in or out of Saudi Arabia and are subject to declaration. These Implementation Rules are not expected to be released until late November 2003, and we have not been able to review them.

We have no KSA Law that purports to detect or monitor the physical cross-border transportation of currency or negotiable instruments.

We have no KSA Law that purports to require financial institutions to report currency transactions above a certain threshold, to a national central agency.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

⁹⁶ FATF Recommendation 19. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

No information is available on any Saudi government efforts regulate the flow of cash and precious metals. The Implementation Rules will guide implementation and enforcement. Without them, it is even uncertain which authorities will be responsible for enforcement in this area. It should be noted, though, that much of the AML-CTF regime's regulatory apparatus can be avoided by physically moving funds in cash. Currency smuggling is common in the Middle East.⁹⁷ Border controls are weak and economies are cash-based. Money or readily convertible commodities such as gold or gemstones can be moved using routes and methods commonly employed by criminal organizations.

⁹⁷ Greenberg et al. *Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations* (2002), 16.

Principle 55: Monitoring of Wire Transfers

Standard:

In order to detect the use of wire transfers for terrorist financing purposes, financial institutions should ensure that accurate and complete information on the originator and the beneficiary of the wire transfer is recorded and included with the wire transfer through the entire chain. Enhanced scrutiny and monitoring of suspicious activity pertaining to funds transfer not containing complete information should be performed.⁹⁸

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

SAMA- AMLCTF, 3.10 requires banks to record and be able to provide the remitter's name, account number, address and the purpose of the remittance for all outgoing transfers. Article 11.1 requires banks to have full information on the remitter's and beneficiary's name, the remitter's address and the account number, and the purpose of the remittance for all incoming and outgoing transfers. Such information should be available upon request.

Neither of the two articles requires enhanced monitoring of the transactions with incomplete information. For this reason, Saudi Arabia is only largely compliant with this principle. Industry business practices recommend the investigation of such occurrences, attempt to collect the missing information, and eventually reporting the suspicious transaction if the information is not available⁹⁹.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

⁹⁸ FATF Special Recommendation VII. The full text of the FATF Special Recommendations on Terrorist Financing is appended to this report in Annex 2.

⁹⁹ Interview with compliance officer at large international bank November, 2003.

Retention of Records

Records of transactions and identification data are necessary documents in order to reconstruct transactions and follow the money trail in an investigation. If such documents are destroyed, not maintained long enough, or are not made available to competent authorities, then the reconstruction of evidence is seriously impaired.

Principle 57: Retention of Records

Standard:

Financial institutions should maintain transaction records and identification data for at least five years. Such records should be readily available to domestic authorities upon request. Industry best practices extend this requirement to non-financial institutions that are involved in financial transactions.¹⁰⁰

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an implementation and enforcement perspective, Saudi Arabia is compliant in terms of financial institutions but we have not been able to verify compliance in terms of non-financial institutions.

Law:

The KSA AMLL Article 5 goes beyond the recommended 5-year period for retention of records both for financial and non-financial institutions, and mandates a minimum of 10 years retention. The type of documents required to be maintained are “all records and documents that explain the financial, commercial and monetary transactions, the files of commercial accounts and correspondence and copies of the ID”.

SAMA-AMLCFT, Article 8 is specific about the documents that should be maintained, but does not specify the retention period for the records under section 8.1, which include records of all customer transactions, account opening documents, customer IDs, and details of customer accounts and balances. Section 8.2 stipulates that certain non-financial documents, including KYC related documents and suspicious activity reports, must be maintained for a period of 10 years.

Saudi Arabia has thus provided for the retention of the appropriate records for an appropriate period. There is some ambiguity, however, in that the KSA-AMLL Article 5 issues a decisive time period over which documents must be preserved, but does not specify precisely which documents. SAMA-AMLCFT, Article 8, which should refine KSA-AMLL Article 5, is specific about documents but in Section 8.1 does not indicate for how long these important documents are to be preserved.

Enforcement:

Saudi Arabia does enforce record-keeping requirements on banks¹⁰¹. We have not been able to verify Saudi Arabia’s compliance with this principle from an enforcement perspective with regard to non-financial institutions.

¹⁰⁰ FATF Recommendation 10: The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

¹⁰¹ Interview with former senior SAMBA employee, November 12 2003

Banks are required to maintain records of transactions and Identification documents, including other KYC related documents. It is not clear how long each type of records must be maintained. We could not verify the implementation/enforcement of this principle by non-financial institutions.

Implementation:

Saudi banks have implemented record-keeping requirements.¹⁰² We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective with regard to non-financial institutions.

¹⁰² Interview with former senior SAMBA employee, November 12 2003

Non-Financial Businesses

Non-financial businesses pose a high-risk of Money Laundering and Terrorist Financing due to a less stringent regulatory environment. Of special concern are sectors that involve the transfer of liquid assets on a large scale. Any flow of liquid assets presents the opportunity for money laundering or for the transfer of funds to terrorists. Such non-financial businesses include, but are not limited to, real estate agents, dealers in precious metals and stones, lawyers, notaries and other independent professionals. For similar reasons, alternative or informal remittance systems are another sector of serious concern.

Principle 57: Regulation and Supervision of Non-Financial Businesses

Standard:

Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations to combat money laundering and terrorist financing.¹⁰³

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely non-compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL covers "Financial and Non-Financial Institutions," defined in Article 1(5) as any establishment in the kingdom engaged in any one or more financial, commercial or economic activity such as banks, money-exchangers, investment companies, insurance companies, commercial companies, establishments, professional firms or any other similar activities set forth in the Implementation Rules.

The SAMA-AMLCFT addresses itself solely to banks. The Saudi Arabia Monetary Agency Law (the "KSA-SAMA") authorizes SAMA to "control commercial banks and persons engaged in the exchange of currencies business" (Article 1(c)). The KSA-BCL, in Article 1, defines a bank as anyone engaged in any banking business, and defines "banking business" as operations of receiving monies as current or fixed deposits, the opening of current accounts and credits, the issue of letters of guarantee, payment and collection of cheques, orders, payment vouchers and other documents having value, discount of bills and promissory notes and other commercial papers, foreign exchange business and other banking business.

From the laws to which we have access, SAMA does not appear to have the authority to oversee entities other than banks and money changers, though we understand that SAMA also regulates the insurance sector and the securities market.¹⁰⁴ Yet even using the expansive definition of "banking business" in the KSA-BCL, this still does not cover alternative remittances conduits. We note that SAMA has made efforts to engage these issues by promulgating rules to banks dealing with charitable organizations and hawaladars, but that is still an indirect and unsatisfactory way of achieving oversight of them.

¹⁰³ FAFT Recommendation 24. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

¹⁰⁴ Interview, Senior U.S. Government official, November 21, 2003.

We also note that the KSA-BCL itself appears to place money changers under a separate regime from banks (Article 2(b)), and we have not seen these institutions addressed in any regulatory framework. We understand that SAMA is in charge of regulating money changers, but we have seen no regulations that apply to them.

We stress the need for oversight of cash-intensive non-bank, non-money changer businesses such as precious commodities dealers, pawnbrokers, travel agencies, and import/export businesses, as well as real estate brokers, lawyers and accountants. Regulated record keeping and due diligence that made it possible to link individuals to specific transactions, as well standards for suspicious transactions and protocols for reporting them, would strengthen the Saudi CTF regime.

The AML/CFT regulatory framework functions as an integrated whole. Even if the KSA-AMLL Implementation Rules are extended to all relevant institutions, Saudi enforcement of those rules will be damaged without the type of thorough, rigorous and professional compliance measures that SAMA has promulgated in the banking sector.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 58: Due Diligence Recommendations Applied to Non-Financial Institutions

Standard:

The same level of due diligence performed by financial institutions should apply to non-financial institutions.¹⁰⁵

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely non-compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Most of the regulations that apply to financial institutions should also apply to Non-Financial Institutions, particularly those NFIs cited by FATF Recommendations 12 and 16. As noted above, the AML/CFT regulatory framework functions as an integrated whole. While the KSA-AMLL applies to NFIs, the SAMA-AMLCFT does not. Even if the KSA-AMLL Implementation Rules *are* extended to all relevant institutions, Saudi enforcement of those rules will be damaged without the type of thorough, rigorous and professional compliance measures that SAMA has promulgated in the banking sector.

We are missing the "Implementation Rules" referenced in the KSA AML. We are also missing any and all relevant regulations imposed by KSA government ministries (esp. the Ministry of Commerce) to address these issues, such as the "Regulations for Companies" or the "Saudi Arabian Auditing Standards."

We have found Saudi Arabia to be only partially compliant with this principle for the following reasons:

a. Ambiguous Scope of the Law

We are concerned with the scope of Saudi law in regard to this principle. The KSA AML Law refers to various forms of Non-Financial Institutions and incorporated entities, companies, establishments, and firms. It is not clear that these categories include proprietorships, precious commodities dealers, or professionals such as lawyers or accountants.

b. Due Diligence

AML 4 covers fictitious names and numbered accounts, but requires verification of a client's identity "at the start of dealing with such client ... *or* upon concluding commercial transactions therewith." [emphasis added] Such timeline stipulation leaves the law vulnerable to exploitation.

It is also vague on verification standards, has no provision for verification of identity upon doubt or suspicion, has no thresholds for closer scrutiny, has no ongoing due diligence, is ambiguous

¹⁰⁵ FATF Recommendation 5, 6, 8-12, 13, 14, 15, & 21 Basel 18,19, 22, 23, 35-36, 41-48, 55-59 and Industry best practices. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

about verifying the control structure and beneficial ownership in a transaction, is silent on understanding “the intended nature” of the business relationship, and has no requirements for action if verification is not successful

There is no discussion of PEPs in the KSA AML, so there may be no additional due diligence or caution on the part of NFIs in dealings with such individuals. Similarly, there is NO discussion of 3rd-party due diligence in the KSA AML, even though FATF Recommendation 12 suggests that most of the recommended due diligence measures be extended to third-parties with which the NFI has dealings.

c. Record-Keeping

AML 5 covers record-keeping but is ambiguous. It goes beyond the required minimum 5 year period for retention of records both for financial and non-financial institutions, and mandates a minimum of 10 years retention. The type of documents required to be maintained are “all records and documents that explain the financial, commercial and monetary transactions, the files of commercial accounts and correspondence and copies of the ID”. The phrase “records and documents that explain the transactions” is ambiguous.

d. Detection and Reporting of Suspicious Transactions

AML 6 & 7, in combination, *might* be construed to cover suspicious transactions, but are extremely vague. Article 6 requires institutions to have in place measures to “detect and foil any of the offences herein.” Article 7 follows this with language referring to “complex unusual large or suspicious transactions.”

AML 7 requires Non-Financial Institutions to immediately notify the FIU and submit a report regarding suspicious transactions. However, this requirement is preceded by the phrase “upon gathering *sufficient* indications and evidence” [emphasis added], without explanation as to what constitutes “sufficiency” in this case.

e. Provision of Information and Safe Harbour

AML 8 stipulates an obligation to provide documents, records, and information – “subject to confidentiality provisions” and “in accordance with applicable regulations.” The secrecy provision, AML 13, provides that “information disclosed by NFI’s *may* be shared with the concerned authorities *if* such information is connected with a violation of these Regulations.” [emphasis added] It is unclear how forthcoming this actually requires NFIs to be.

There appears to be no safe harbour for NFI employees, though as noted above, AML 13 provides that information may be provided in certain circumstances. There is no explicit protection for those who provide the information.

f. Internal Policies and Procedures

AML 10 requires NFIs to develop internal policies, procedures, and controls, as well as ongoing training programs, and internal audit functions. The law is somewhat vague about training requirements and also does not mention adequate employee screening procedure, and makes no mention of external auditors (as per Basel 59). Otherwise, the law is largely compliant on this issue.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have not been able to obtain the necessary data to make an informed assessment.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 59: Alternative Remittances

Standard:

Alternative remittance systems should be licensed and subject to the same level of scrutiny that apply to financial and non-financial institutions..¹⁰⁶

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Overall, Saudi law is ambiguous, conflicted and incoherent on the issue of alternative remittances such as hawala. The status of the business of alternative remittance is not clear under Saudi law, nor is the status of money changers who may carry out this business. It is unclear what regulations, if any, govern this form of money transfer, though it does appear that SAMA has authority for licensing money changers of all types. However, even SAMA's rules are unclear about the status and legality of alternative remittances.

KSA AML Article 1 defines banks to include all natural or legal person who carry on "banking activities," which includes "receiving money on current or fixed deposit account, opening of current accounts, opening of letters of credit, issuance of letters of guarantee, payment and collection of cheques, payment orders, promissory notes and similar other papers of value, discounting of bills, bills of exchange and other commercial papers, foreign exchange transactions and other banking business." This appears to include part of the money changing business; as noted above in Principle 25, however, it is not clear that this includes alternative remittance conduits.

We also note that the KSA BCL appears to place money changers under a separate regime from banks (Article 2(b)), and KSA Banking Control Law Article 2b limits the business of money changers to the "exchange of currency." However, this appears to conflict with the Regulations for Money Changing Business Article 3b, which stipulates that "the Saudi Arabian Monetary Agency may license any money-changer to make *cash remittances* inside and outside the Kingdom." [Emphasis added.] It is not clear that such money-changers are subject to the SAMA Rules Governing AML, or any other such regulations, since the KSA BCL Article 2b does not appear to recognize such remittances by money changers as "banking business."

We have not seen these institutions addressed in any substantial regulatory framework. We understand that SAMA is in charge of regulating money changers, but other than the Regulations for Money Changing Business, which do not address AMLCTF, we have seen no rules that apply to them. SAMA has no visible directives pertaining to the control of the initial transaction, no

¹⁰⁶ FATF Special Recommendation VI: The full text of the FATF Special Recommendations on Terrorist Financing is appended to this report in Annex 2.

discussion of how to monitor the settling of claims across hawala networks, and no regulations on the methods of practice of hawala. Although this level of detail in the regulation of the hawala system may exist in the KSA, no information regarding these details has been made available. If this level of detail does not exist, then this remains a serious vulnerability of the Saudi financial system to money laundering and terrorist financing, one in which the KSA is well behind other countries in its regulatory establishment.

KSA Banking Control Law Article 2 renders unlicensed *banking* activities to be illegal, and SAMA Rules Governing AML Article 9 defines “unlicensed” or “unauthorized” alternative remittances to be illegal, and movement of funds for such purposes to be considered a “suspicious transaction.” However, although “authorized” hawala appears to be legal under the Regulations for Money Changing Business, the SAMA-AMLCFT Article 5.1.8 decrees that banks should not allow accounts that are used for *any* alternative remittances such as hawala, and should report such activity as “Suspicious Activities.”¹⁰⁷ [Emphasis added.] As such, SAMA’s position on alternative remittances appears inconsistent. It should be noted that the Regulations for Money Changing Business, promulgated in 1981, declares a moratorium on new licenses for money changing businesses.

Implementation / Enforcement:

In practice, there are some nine organized “money houses” licensed to carry out remittances, as well as some number of licensed “money-changers” who are *not* permitted to carry out remittances. To our knowledge, therefore, there are no licensed individual hawaladars, and as such there should *be* no individual hawaladars, and no new exchange houses or individual money changers should have opened for business since 1981.

Informal funds transfer systems such as hawala are a major element of wealth movement in and out of the Kingdom of Saudi Arabia, and may well be the largest method by which money enters and leaves the KSA. There are multiple forms of hawala, including single-hawaladar operations (where the individual or entity has multiple international bank accounts) and hawaladar-network (where multiple individuals or entities operate across an international network) operations. Each has its own vulnerabilities to exploitation by money-launderers and terrorism financiers, and each poses different challenges to regulators.

We have been unable to verify the enforcement of the licensing restrictions, which have been in place since at least 1981. Data on unlicensed remittances is notoriously difficult to acquire. However, it appears that the Saudi government has not succeeded in fully regulating alternative remittances, judging by the continued existence of hawaladars outside the licensed exchange houses.¹⁰⁸ It is also unclear how the money changing business has sustained itself in the 23 years since the Regulations for Money Changing Business required SAMA to stop issuing licenses for money changers.

SAMA, in the May 2003 rules for AMLCTF, has made suggestions to banks on how to identify hawaladars of the first variety (single-entity, multiple-account operations). However, since the main financial transfer mechanism of these operations lies outside the KSA, this measure may be largely ineffective if it is not accompanied by a coordination of efforts between Saudi Arabia and

¹⁰⁷ SAMA, *Rules Governing Anti Money Laundering and Combating Terrorist Financing*, May 2003, Article 5.1.8.

¹⁰⁸ Interview with Sheikh Hamad Al-Sayari (governor of SAMA), “Strength to strength,” *The Banker*, October 2002.

other countries to control and monitor inter-account transfers. Given the tight control and overall opacity and secrecy that permeates the Saudi financial sector, there is reason to question the extent to which this level of international coordination can occur. With respect to the second variety of hawala, the multiple-intermediary form, there appears to be no discussion of how to address this type of operation.

Conclusion – Regulatory Regime

Our review and analysis of Saudi Arabia’s AML-CFT Regulatory Regime has highlighted a number of areas in which that system is fully or substantially compliant with relevant international standards. Saudi Arabia has made important strides in creating an effective infrastructure for combating money laundering and terrorist financing, including enacting legislation, establishing supervisory, reporting and enforcing bodies, and mandating the creation of efficient internal policies and procedures for financial and non financial institutions. The laws and regulations dealing with customer due diligence, transaction monitoring, and retention of records are largely adequate. However, there are also several issues of concern, which will require continuing attention:

1. The Regulatory Infrastructure may not be effectively implemented. Saudi Arabia’s secrecy laws may impede the full implementation of the International Standards and industry best practices in the areas of collaboration between regulatory and enforcement bodies and international cooperation. There is no reliable information regarding the country’s financial and human resources in regulatory and enforcement capacity, including the level of training of employees of financial and non-financial institutions, law enforcement agencies and regulatory bodies. There are no provisions in the law for the screening of employees in order to ensure the highest standards of moral conduct of the employees in critical positions with respect to money laundering and terrorist financing. The level of implementation of AML and CTF policies in foreign branches and subsidiaries might not be the same as the standard established in Saudi Arabia. In addition, there is concern regarding the functionality of the newly created FIU and its role in effectively analyzing suspicious activity reported by financial and non-financial institutions.

2. The customer due diligence might be inadequate with respect to certain categories of customers. We are missing SAMA circulars and Implementation Rules dealing with customer identification and due diligence, therefore we could not fully assess the compliance with the standards. The provisions of the laws dealing with Politically Exposed Persons do not specifically cover the royal family, and do not require an evaluation of the source of wealth. The laws also lack due diligence elements with respect to Correspondent Banking, and are inadequate with respect to special purpose vehicles and trusts.

3. Due to Saudi Arabia’s lack of transparency, the implementation and enforcement of transaction monitoring cannot be reasonably assessed. The FIU is not fully functional. We do not know if it is able to process and act on reported suspicious transactions. We have no information about the monitoring of transactions by non-financial institutions. We have no information regarding the monitoring of cash transactions. The threshold for monitoring transactions is higher than industry best practices and FATF recommendations (USD 26,660 versus USD 15,000). The procedures and standards for enhanced monitoring of unusual transactions or transactions with incomplete information are not clear or are not available. Transactions with countries with lax AML controls are not subject to enhanced scrutiny, except for the NCCT countries.

4. The regulation and supervision of non financial businesses may be substantially inadequate. Other than the largely inadequate KSA-AMLL, we were unable to obtain any significant legislation dealing with AML-CTF in non financial business sectors. We also could not obtain significant information regarding the implementation and enforcement of the AML and CTF regulations. Some of the legislation dealing with non financial businesses and alternative remittance systems is new, and the implementation and enforcement may not have been fully completed as yet. Particularly with respect to alternative remittance systems, the laws we were able to obtain are unclear, contradictory, and in need of substantial revision and clarification.

Non-Profit Sector (Charities)

To assess the effectiveness of Saudi Arabia's regulations in combating terrorist financing through charities, we have performed a step-by-step comparison of Saudi Arabia's laws with the international best practices outlined by the FATF memo "Combating the Abuse of Non-Profit Organizations," issued October 11, 2002. These best practices are broadly divided into four areas of focus, which include financial transparency, programmatic verification and administrative and oversight bodies. We will examine Saudi Arabia's regulatory regime in each of these areas.

Financial Transparency

Financial transparency guarantees that charitable organizations maintain documentation that accounts for all their programs. To insure the transparency of charitable operations, independent auditing is an efficient and widely recognized method of ensuring that accounts of an organization accurately reflect the reality of its finances.

1. Principle 60: Financial Accounting Transparency

Standard:

Non-profit organizations should maintain and be able to present full program budgets that account for all program expenses. These budgets should indicate the identity of recipients and how the money is to be used. The best practices do differentiate between administrative and program budgets and require both to be protected from diversion.¹

Assessment:

From a legal perspective, the relevant Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the 1981 Regulations Regarding Charities requires all charities to “keep a record of all financial statements, budgets, and money raised, its sources and how it is spent.”²

Enforcement / Implementation:

Saudi Arabia's regulations in this area meet the standards outlined by the FATF. In some respects, Saudi Arabia's regulations go further than international best practices. By requiring charities to keep a record of their budgets and expenses and consolidate all of their accounts into a single account that is strictly controlled, the Saudi Arabia's regulatory regime provides a mechanism for authorities to monitor the finances of charities.

¹ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

² *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Principle 61: Independent Auditing

Standard:

Independent auditing is a widely recognized method of ensuring that accounts of an organization accurately reflect the reality of its finances and should be considered a best practice. Where practical, such audits should be conducted to ensure that such organizations are not being used by terrorist groups. It should be noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.³

Assessment:

From a legal perspective, the relevant Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

According to Article 16 of the 1981 Regulations Regarding Charities, the MLSA has “the right to review all files and registers. If an MLSA officer presents himself and requests information about the association, the association must provide this officer with such information.”⁴

Enforcement / Implementation:

A large loophole with regards to the financial accounts of charities is the lack of regular and independent audits. Though the 1981 Regulations Regarding Charities states that the MLSA has “the right to review all files and registers,” it does not require any regular inspections. Also, an audit performed by a MLSA officer would not be considered truly “independent” since the MLSA is the regulatory body for all charities in Saudi Arabia.

In the Green Book and other recent reports, Saudi Arabia has claimed that it has performed full audits of all its charities – “Since September 11, all charitable groups have been audited to assure that there are no links to suspected groups.”⁵ However information about these audits has not been made public. It is not clear who performed the audits, what standards were used and what the specific results were. Also, these reviews may not have examined the foreign operations of Saudi Arabian charities.

³ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

⁴ *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

⁵ *Initiatives and Actions in the Fight Against Terrorism*, The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 62: Registered Bank Accounts

Standard:

It is considered a best practice for non-profit organizations that handle funds to maintain registered bank accounts, keep its funds in them, and utilize formal or registered financial channels for transferring funds, especially overseas.⁶

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

The new SAMA regulations passed in May of 2003 require banks and money-changers to require depositors to provide them with identification and other required information for verification before accepting deposits from charities. In addition, "all bank accounts of charitable or welfare societies must be consolidated into a single account for each such society."⁷ Going beyond the international standards, Saudi Arabia has banned its charities from transferring any funds abroad and requires charities to receive permission from SAMA to open a bank account. In addition, new regulations place strict controls of the bank account of charities, preventing such transactions as cash withdrawals and credit card usage.

Enforcement / Implementation:

One potential loophole is the hawaladars or money changers who often operate with little regulatory oversight in Saudi Arabia. Though they technically fall under the jurisdiction of SAMA, according to one expert on the Saudi Arabia's financial sector, it has proven difficult for the authority to exert control over the network of money changers that dot the country.⁸ Many do have the required licenses but many of these hawaladars do not keep detailed records and do not have the internal controls of a bank. Thus, it appears to remain relatively easy for a charitable organization within Saudi Arabia to open up an account with a money changer without the permission of SAMA and transfer funds under the radar of the monetary authority.

Another weakness of the new regulations is the lack of oversight over individuals who may be funneling funds to terrorist organizations abroad. Some experts have argued that individuals, not charities, are the largest contributors to terrorist organizations like Al Qaeda. **Brisard**, for instance, noted that the Golden Chain list found in the offices of Benevolence International Foundation, a charity operating in Sarajevo, was composed of the top 20 Saudi financial sponsors of Al Qaeda. All of them were individuals and they had a cumulative net worth of \$85 billion or 42% of the Saudi annual GNP.⁹ The new regulations do not put a stop to the flow of funds from wealthy individuals like these, who can still easily open up bank accounts and make transfers abroad.

⁶ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

⁷ Saudi Information Office, Press release, June 12, 2003

⁸ Interview with Saudi banking expert November 2003

⁹ Jean-Charles Brisard testimony to the Committee on banking, housing and urban affairs U.S. Senate October 22, 2003

Also, since Saudi Arabia has no capital controls, any charity, group or individual could simply carry an unlimited amount of cash out of the country. In fact, the practice of physically moving cash abroad is so well-established in Saudi Arabia that there are courier services that specialize in cash deliveries to international financial centers like Dubai.

Finally, it appears that it remains possible for individuals who seek to donate to illegitimate organizations with charity fronts abroad to transfer funds abroad through their own accounts or by creating new ones, both in Saudi Arabia and abroad. In addition, even with new regulations placing strict controls on charitable funds, Saudi Arabian charities outside of the country have continued to operate, raising the question of how this is possible.

Programmatic Verification

Programmatic verifications encompass the solicitation of information regarding the donors and the beneficiaries of charitable donations. These verifications should be implemented periodically by transparent and credible authorities to insure the application of best practices and the non misuse of charitable organizations domestically and abroad.

Principle 63: Transparent Solicitation

Standard:

Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organization should then ensure that such funds are used for the purpose stated.¹⁰

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no regulations regarding the solicitation of donations in the Kingdom. However, in May of 2003, the Ministry of Labor and Social Affairs banned all donation-boxes in mosques.

Enforcement / Implementation:

Donation boxes have been a particular problem in Saudi Arabia in terms of combating terrorist financing. Funds collected in donation boxes are distributed by mosques to various individuals and groups with little oversight of these distributions.

In recent months, during investigations into the Riyadh bombings, a clear link was identified between these donation boxes and Al-Qaeda. The *Jedda Arab News* reported on September 17th, “in raids on a small farm and a rest house in Riyadh as well as locations in Qasim and the Eastern province, security forces seized rocket-propelled grenades, explosives and detonators as well as night-vision binoculars, monitoring cameras, computers, fake passports and ID cards and *collection boxes*.”¹¹

Consequently, Saudi Arabia has moved to curtail *zakat* through donation boxes. An article in the *Jedda Arab News* quoted Interior Minister Prince Naif as warning “people to be wary of putting money in collection boxes found at the entrance to some mosques. ‘Those wishing to contribute must verify where the money will go,’ he said. He urged Saudi citizens, ‘not to contribute unknowingly to the killing of people by paying money to suspicious boxes or parties.’”¹² And in August of this year, the Ministry of Labor and Social Affairs banned the collection of cash through donation boxes placed in mosques, schools and shopping malls. However, Western experts on Saudi Arabia have recently reported that even after the ban, these boxes continue to be placed in mosques and other areas.¹³

¹⁰ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

¹¹ The *Jedda Arab News* article 17 September 2003

¹² The *Jedda Arab News* article 17 September 2003

¹³ Interview with Saudi banking expert November 2003

Some experts have pointed out that Saudi Arabia has made several previous attempts to regulate its charities – to no avail. Brisard testified that there have been many regulations including the 1976 Fundraising for Charitable Purposes Regulation and the 1994 royal decree banning the collection of money in the Kingdom for charitable causes without official permission. But he noted, "through these various unsuccessful attempts to regulate or control the recipients of *zakat* or donations, one must question the real ability and willingness of the Kingdom to exercise any control over the use of religious money in and outside the country."¹⁴

¹⁴ Jean-Charles Brisard testimony to the Committee on Banking, Housing and Urban Affairs U.S. Senate October 22, 2003

Principle 64: Programmatic Oversight

Standard:

To help ensure that funds are reaching the intended beneficiary, non-profit organizations should ask the following general questions:

Have projects actually been carried out?

Are the beneficiaries real?

Have the intended beneficiaries received the funds that were sent for them?

Are all funds, assets, and premises accounted for?¹⁵

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no Saudi regulations requiring charities to report on whether projects have been carried out, whether the beneficiaries are real and whether they received the funds that were sent to them. However, the 1981 regulations do require charities to keep records of all of their correspondence, their funds and financial statements and requires charities to send the minutes of all of their meetings to the MLSA within 10 days of the meeting (Article 8d).¹⁶

Enforcement / Implementation:

This is the point of greatest weakness in Saudi Arabia's anti-terrorist financing regulatory regime. By and large, Saudi Arabian regulations regarding programmatic verification do not meet the standards outlined by FATF. These standards require charities to declare the purpose of all solicitations and ensure that the funds are used exclusively for the stated causes and by the groups for which the funds were donated. There are currently no Saudi Arabian laws addressing solicitations in the kingdom and little oversight of how donated funds are used by the charities. Though the 1981 Regulations do require charities to keep records of all of their correspondences, funds and financial statements, they does not specifically oblige charities to account for all of the funds they raise and whether projects are really carried out.

Complicating the issue of donations in Saudi Arabia is the practice of *zakat*. As mentioned above, *zakat* is a requirement for all financially-able Muslims and can be donated in many forms – to the charities or the needy themselves, through the government which collects a *zakat* tax or until they were banned, through donation boxes in mosques and other areas. Anonymous donations are considered particularly pious and those giving *zakat* are usually not interested in how their donations are spent. They are simply interested in the act of giving *zakat*, which meets the religious requirement. Thus, charities and others receiving donations in Saudi Arabia have traditionally had little accountability to their financial backers, including the government.

¹⁵ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

¹⁶ *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Zakat taxes are collected and controlled by the Department of Zakat and Income taxes (Directorate General of Zakat & Income Tax (DZIT)) of the Saudi Ministry of Finance and National Economy.¹⁷ These donations usually take the form of bank transfers to the more than 240 charities. Though the department has strict instructions for organizing, auditing, and collecting *zakat* from all Saudis obligated to pay, it has had little guidance on how these funds should be distributed. Also, there are no regulations regarding the oversight of these funds once they are received by the charities. Thus, charities in the kingdom have been and are still receiving billions of dollars from the government without public accountability of where these funds are going.

¹⁷ http://www.mof.gov.sa/e_alzakah.html

Principle 65: Field Auditing

Standard:

Direct field audits of programs may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists. However, non-profit organizations should track program accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted.¹⁸

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no regulations requiring field audits for charities in Saudi Arabia. However, as mentioned above, the MLSA has the right to demand and review all the files and registers of charities.

Enforcement / Implementation:

A large loophole with regards to the financial accounts of charities is the lack of regular and independent audits. Though the 1981 Regulations Regarding Charities states that the MLSA has “the right to review all files and registers,” it does not require any regular inspections. Also, an audit performed by a MLSA officer would not be considered truly “independent” since the MLSA is the regulatory body for all charities in Saudi Arabia.

In the Green Book and other recent reports, Saudi Arabia has claimed that it has performed full audits of all its charities – “Since September 11, all charitable groups have been audited to assure that there are no links to suspected groups.”¹⁹ However information about these audits has not been made public. It is not clear who performed the audits, what standards were used and what the specific results were. Also, these reviews may not have examined the foreign operations of Saudi Arabian charities.

¹⁸ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

¹⁹ *Initiatives and Actions in the Fight Against Terrorism*, The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 66: Foreign Operation Oversight

Standard:

Where possible, a non-profit organization should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.²⁰

Assessment:

From a legal perspective, Saudi Arabia is partially in compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no specific laws or regulations that empower the government of Saudi Arabia to oversee the operations of its charities outside of the country. However, the 1981 Regulations state “charities cannot open subsidiaries without the permission of the MLSA.” In addition, the SAMA regulations issued in May of this year do allow the government to control how much money domestic Saudi charities are sending abroad.²¹

Enforcement / Implementation:

The new regulations restrict charities from transferring any funds abroad without authorization from SAMA. This is another key regulatory issue for Saudi Arabia. Its charities’ foreign operations are wide-ranging and have often been accused as serving as the points of delivery of funds to terrorist organizations. For instance, the Saudi-supported World Assembly of Muslim Youth operates in 55 countries while the International Islamic Relief Organization, another organization backed by Saudis, is reputed to have offices in over 90 countries. Both have been charged in the media with “passing on money” to terrorist organizations.²² Both deny involvement and cite a large number of legitimate charitable projects.

Though limited, Saudi regulations of charities’ foreign operations go further than FATF recommendations, which only state that “the competent authorities in both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work.” The 1981 Regulations require charities to get permission from the MLSA before opening any subsidiaries. However, this area remains a vague in terms of legal authority and enforcement.

²⁰ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

²¹ *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

²² Interview with Saudi banking expert November 2003

Principle 67: International Cooperation

Standard:

When the home office of the non-profit organization is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages.²³

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

We found no specific law relating to this matter. However, according to a Saudi Embassy press release on October 18, 2002, Saudi Arabia and the U.S. maintain a counter-terrorism committee comprised of intelligence and law enforcement personnel who meet regularly to share information and plan actions to curb terrorism financing.²³

Enforcement / Implementation:

Information sharing among government agencies is critical to the efforts to tackle terrorism financing. The global aspect of many terrorist groups is imposing a new reality on government agencies: the need for further international cooperation. Al-Qaeda is a stunning example of a terrorist group able to plan and coordinate its operations worldwide efficiently. While much of the information collected by single government agencies can be of significant value in terrorism financing investigations, the value will not be realized nor maximized absent the ability to share it with other agencies worldwide.

The establishment of the U.S- Saudi Joint Task Force in the wake of the terrorist bombings in Riyadh on May 12, 2003 is an important step toward further international cooperation between the U.S. and Saudi agencies. Through this initiative, the FBI and the Internal Revenue Service (IRS) have officials stationed in Saudi Arabia to search individuals and charities bank accounts and computer records for links to terrorism. This is also an opportunity to join linguistic, computer, and forensic talents in the fight against terrorism.²⁵

Because of these uncertainties, it is crucial to increase cooperation between U.S. and Saudi agencies in charge of monitoring charities to track their finances and their uses both in Saudi Arabia and abroad. In addition, better coordination in the Joint Task Force can help make up for some deficiencies in the current oversight of charities. On October 2003, Saudi officials unveiled what it called a new manual on the charities regulation, which in large part was based on the Charities

²³ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

²³ Saudi Embassy in Washington Press release October 18, 2002

²⁵ Saudi Embassy in Washington, Press release, August 26, 2003

Regulation Act of 1981. In both cases, the issue of whose responsibility it is to oversee Saudi charities operating abroad is not clear. This leaves a major gap between theory and reality that can be filled through U.S- Saudi cooperation.

In addition to sharing information regarding charities operating in KSA, Saudi authorities could also provide their U.S. counterparts with information related to Saudi charities established in the U.S. This would greatly benefit ongoing investigations by U.S. agencies into Saudi charities operating in the U.S. One example where cooperation would have been crucial involved the Saudi charity International Islamic Relief Organization (IIRO) based in the U.S. under the name International Relief Organization (IRO.) The IIRO was part of an FBI investigation that unraveled a series of Saudi-sponsored charities in Northern Virginia that are linked to Al-Qaeda and its offshoots.²⁶

According to an affidavit filed by the Bureau of Immigration and Customs Enforcement, the IRO invested \$3.7 million in BMI Inc. a private Islamic investment company established in New Jersey that may have passed the money on to terrorist groups. The affidavit contends that the IRO originally received \$10 million from Saudi Arabia in 1991. The money was then used to set up a shell company called Sana-Bell, Inc which was responsible for investing it. According to the affidavit, between 1992 and 1998 Sana-Bell gave \$3.7 million to BMI. A few years later the funds invested in BMI disappeared. The case of IRO is a classic example of how there is a need for enhanced U.S. Saudi cooperation and how that can benefit such investigations.²⁷

International cooperation between U.S and Saudi agencies have produced some concrete results, including freezing the accounts of the Al-Haramain Islamic Foundation and shutting down its branches in Bosnia and Somalia in March 2002. While the Saudi headquarters for this private charitable entity is dedicated to promoting Islamic teachings, U.S and Saudi agencies determined that those specific branches of Al-Haramain were engaged in supporting terrorist activities and terrorist organizations such as Al-Qaeda, AIAI (al-Itihaad al-Islamiya), and others.²⁸

The United States and Saudi Arabia have also jointly taken action to freeze the assets of a Saudi citizen who headed an organization allegedly giving financial support to Al-Qaeda. In September 2002, the U.S. and Saudi Arabia designated Wa'el Hamza Julaidan, director of the Rabita Trust and other organizations, as a person who supports terrorism.²⁹

²⁶ Emerson, Steven and Levin Jonathan, Testimony before the U.S. Senate Committee on Governmental Affairs, July 31, 2003

²⁷ Farah, Douglas, Terrorist funding affidavit, The Washington Post, August 20, 2003

²⁸ U.S. Department of State press release, March 11, 2002

²⁹ U.S. Department of State press release, September 6, 2002

Administration

The transparent administration of the day to day operations of charities and the accountability of their management should be a top priority of charities' oversight agencies. The charities' Board of Directors and employees should act with diligence and probity in carrying out their duties.

Principle 68: Administrative Documentation

Standard:

Non-profit organizations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.³⁰

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

The 1981 Regulations require charities to “announce the names of the board of directors and the organizational chart” (Article 1f). The organizational chart should include, among other information required by Article 5, the goals of the charity, the budget and allocation of finances, information about subsidiaries such as their mission and their relationship with the parent charity. Thus, such information would be sufficient to document the administrative, managerial and policies of the charities’ operations. In addition, charities must report all changes to the organizational chart, which must be forwarded to the MLSA for authorization (Article 3b).³¹

Enforcement / Implementation:

With regards to laws regulating the administrative operations of charities, Saudi Arabia is mostly in compliance with the international standards set by FATF. The 1981 Regulations require charities to document their organizational charts, their board of directors and goes so far as to require that minutes of all meetings be submitted to the MLSA.

³⁰ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

³¹ *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Principle 69: Charity Leadership Accountability

Standard:

The directors or those exercising ultimate control over a non-profit organization need to know who is acting in the organization's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organizations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.³²

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

As stated above, charities are required by the 1981 Regulations to announce the names of its board and founding members.

Enforcement / Implementation:

Documentation of charity leadership is required and full. However there are no regulations Regarding the activities of a charity's partner organizations.

³² Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002.

Principle 70: Charity Leadership Responsibility

Standard:

Directors should act with diligence and probity in carrying out their duties. To this end, directors have responsibilities to the organization and its members to ensure the financial health of the organization and that it focuses on its stated mandate. Directors are also responsible for those with whom the organization interacts, like donors, clients, suppliers and all levels of government that in any way regulate the organization.

These responsibilities take on new meaning in light of the potential abuse of non-for-profit organizations for terrorist financing. If a non-profit organization has a board of directors, the board of directors should:

- Be able to identify positively each board and executive member
- Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings
- Formalize the manner in which elections to the board are conducted as well as the manner in which a director can be removed
- Ensure that there is an annual independent review of the finances and accounts of the organization
- Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organizations;
- Ensure an appropriate balance between spending on direct program delivery and administration;
- Ensure that procedures are put in place to prevent the use of the organization's facilities or assets to support or condone terrorist activities.³³

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

Charities are required by the 1981 Regulations to announce the names of its board and founding members. In addition, the 1981 Regulations require charities to keep records of all of their correspondences, the minutes of all of their meetings and all of their financial transactions (Article 11). As for the board, the 1981 Regulations set out strict standards on various aspects of the board of directors- election must be held by secret ballot, board of directors have 4 year term limits, 90 days prior to election, the MLSA must receive a list of candidates (Article 8).

Enforcement / Implementation:

There are no requirements for annual independent reviews, financial controls, nor for an appropriate balance between spending on direct programs and administration. Most important, neither in the

³³ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002.

1981 Regulations or the SAMA regulations issued earlier this year, are there requirements for procedures that prevent the charity from being manipulated for terrorist financing.

Oversight Bodies

Authorities should have a clear strategy in supervising charities and overseeing their operations. Since many agencies are involved in the oversight practice, there is a need for separation of roles and duties to insure that the control and supervision are implemented in an efficient and professional way.

Principle 71: Law Enforcement Involvement

Standard:

Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organizations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organizations.³⁴

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

Saudi Arabia has set up a Financial Intelligence Unit that is working to combat against the abuse of charities by terrorist groups. In addition, Saudi secret police and the Money Laundering Section of the Drug Control Office have for many years had oversight of money laundering and other suspicious financial transactions in the country.

Enforcement / Implementation:

As discussed above, by and large, Saudi Arabia has most of the regulations in place to properly combat the abuse of charities for terrorist financing. The question remains how all of these different circulars, royal decrees and ministry regulations will work together, which ministry or authority ultimately has jurisdiction over charities and whether all of these regulations are implemented properly.

³⁴ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 72: Specialized Government Regulatory Bodies

Standard:

In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organizations. Specifically, terrorist financing experts should work with non-profit organization oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.³⁵

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: It is not clear whether there has been much interagency outreach and discussion within the government on the issue of terrorist financing. There are no regulations calling for cooperation among the many government agencies that oversee the non-profit sector – the MLSA, the Ministry of Islamic Affairs, the FIU, the High Commission, etc.

Enforcement / Implementation:

There is no centralized authority overseeing charities –the Ministry of Labor and Social Affairs, the Ministry of Interior, the Ministry of Islamic Affairs and SAMA each appear to have their own regulations regarding charities. For example, the Ministry of Labor and Social Affairs supervises charity associations but each charity is also required to have audit committees that must answer to the Ministry of Islamic Affairs.

Although the 1981 Regulations clearly state that the MLSA has jurisdiction over charities, the website of the MLSA contains no information at all regarding charities. In addition, recent Saudi press releases cited the Interior Ministry as the agency dealing with charitable organizations. And through the anti-money laundering regulations passed earlier this year, SAMA also has jurisdiction over the charities through their financial accounts.

The discrepancies in the number of registered charities illustrate the disorganization of the MLSA. According to the Kingdom's Charities Report issued by the Saudi government on April 21, 2002, there are 232 registered charities in the Kingdom but the MLSA simultaneously maintains other documents stating that there are only 194 registered charities (see annex).³⁶

A further complication is the foreign subsidiaries of Saudi charities. Jurisdiction over these operations is ambiguous. It is not clear if the subsidiaries of Saudi Arabian charities operating outside of the Kingdom are subject to the regulations enforced on domestic operations. The terms “foreign” or “domestic” are not mentioned at all in most Saudi regulations and the Green Book mentions that the Ministry of Foreign Affairs (MFA) is involved in the oversight of Saudi charitable operations abroad. Yet questions remain on how the Ministry specifically monitors these operations,

³⁵ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

³⁶ *Kingdom's Charities Report* issued by the Saudi government on April 21, 2002

under what regulatory framework and whether it has any jurisdiction over operations that are taking place outside of their territory.

According to a current US government official, the Ministry of Islamic Affairs authorizes the activities of Saudi Arabian charities overseas.³⁷ The official claims that before opening offices overseas, Saudi charities are required to receive permission from the Ministry of Islamic Affairs. In our research we could not find any documentation about Ministry of Islamic Affairs duties in regards to charities. We were not able to access the website for the Ministry of Islamic affairs, Islam.org.sa, due to the website being password protected. This was the only Saudi government website we found to be password protected. There may not be a contradiction between Ministry of Foreign Affairs foreign oversight and Ministry of Islamic Affairs oversight; however, the lack of any public legislation, the lack of clear mandates to charities to register foreign programming (as opposed to foreign office existence) and the lack of clear institutional authority structures suggest that this is an area of oversight that remains in need of improvement.

FATF suggests that “there should be interagency outreach and discussion within governments on the issue of terrorist financing” (p. 5). At the moment, there doesn’t seem to be much outreach or coordination among all the government agencies involved in the regulation of charities in the Kingdom.

The High Commission with oversight of charities was created earlier this year. As the Green Book states, “Saudi Arabia has established a High Commission for Oversight of all Charities(HCOC), contributions and donations.³⁸ In addition, it has established operational procedures to manage and audit contributions and donations to and from the charities, including their work abroad.” But it is not yet clear what role this new body will actually play and how it will interact with the other ministries. Will it be a clearinghouse for all of the regulations? Or will it simply be yet another government body

There is a crucial role for the HCOC to play. A central body is badly needed to coordinate efforts to regulate charities. There is also a need to increase the transparency of the regulatory process; improve the system for appealing decisions made by regulators; and introduce a range of penalties for non-compliance with legal requirements. A thorough preventive regime would also ensure that charities are satisfying their legal obligations and operating for charity purposes. It is unclear whether this task is being done.

³⁷ Interview with current U.S. government official November 2003

³⁸ *Initiatives and Actions in the Fight Against Terrorism*, The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 73: Government Bank, Tax, and Financial Regulatory Authorities

Standard:

While bank regulators are not usually engaged in the oversight of non-profit organizations, the current political environment underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules, etc – in the fight against terrorist abuse or exploitation of non-profit organizations.³⁹

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: Part of the anti-money laundering regulations SAMA issued in May of 2003 specifically target charities and through these regulations, the monetary authority does have significant oversight of non-profit organizations within Saudi Arabia. Thus, these regulations not only meet, but in some areas, even go beyond, the international best practices

Enforcement / Implementation:

See Enforcement / Implementation of Oversight Principle 13.

The MLSA charities list supplied in the annex of this report makes clear that more than 70% of Saudi charities deposit their funds at the Al Rajhi Bank, a Saudi Islamic bank. Most Saudi charities are based upon religious principles and so might be expected to choose to process their financial operations through an Islamic bank. Al Rajhi Bank is now being investigated for possibly supporting Osama bin Laden and his Al-Qaeda terrorist network⁴⁰. Though the special relationship between Saudi charities and the Al Rajhi Bank raises questions regarding the potential role that Islamic financial institutions in Saudi Arabia play in terrorism financing, it also provides bank regulators an opportunity to oversee the collection and disbursement of a significant percentage of Saudi Arabia's charitable funds

³⁹ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

⁴⁰ The Atlanta Journal-Constitution, Nov 16th, 2003

Principle 73: Tax Authority Participation

Standard:

In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.⁴¹

Law: Saudi Arabia does not tax its charities, thus it would not be able to implement this best practice.

Enforcement / Implementation:

This standard is not applicable to Saudi Arabia.

⁴¹ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 74: Information Sharing

Standard:

Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organizations by terrorist groups or supporters is shared as appropriate.⁴²

Assessment:

From a legal perspective, this is not applicable.

From an implementation/enforcement perspective, this is not applicable.

Law:

Since Saudi Arabia does not tax its charities, it would not be able to implement this best practice.

Enforcement / Implementation:

This standard is not applicable to Saudi Arabia.

⁴² Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 75: Private Sector Watchdog Organizations

Standard:

In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organizations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organizations by terrorists. Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organizations in their attempt to put best practices into place for combating the misuse of non-profit organizations.⁴³

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: In Saudi Arabia, the MLSA acts as the non-profit sector's watchdog and accreditation organization.

Enforcement / Implementation:

There are few private-sector organizations that have the capacity or knowledge of best practices for combating the misuse of non-profit organizations.

Oversight Bodies Conclusion: In theory, there appear to be many government agencies in charge of regulating and supervising charities. In reality, the role of these agencies is unclear and sometimes, there is overlap which creates bottle necks and major bureaucratic delays.

⁴³ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Sanctions

Sanctions are coercive actions taken by the oversight agencies to insure that the regulation in place is well respected. A battery of sanctions ranging from simple financial fines and penalties to imprisonment should allow the charities' oversight agency to conduct its mission and deter any action that is contradictory with the regulation in place.

Principle 76: Legal Accountability

Standard:

Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.⁴⁴

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is not in compliance.

Law: Through SAMA, Saudi Arabia has established new regulations for those who misuse charities for terrorist financing. However, we have been unable to access these new regulations.

Enforcement / Implementation:

Further complicating efforts to regulate charitable contributions, members of the Saudi royal family have traditionally been immune to many of the laws and regulations issued by the Kingdom of Saudi Arabia. Lack of compliance among royal family members with regulations issued by the government form another obstacle to thorough and transparent regulatory regimes.

Some have accused the Saudi government itself of having donated to terrorist organizations. A document released to the press by the Israeli government and reportedly seized from Hamas offices in Gaza cites Hamas official Khaled Mashaal thanking the Saudi government for continuing "to send aid to the people through the civilian and popular channels, despite all the American pressures exerted on them." The official is reported to have sent the letter after meeting with Crown Prince Abdullah in October of 2002.⁴⁵ However, the AP report makes clear that "Saudi officials say their government's support for Palestinian causes, about US\$80-million to US\$100-million a year, goes solely to the Palestinian Authority, and that money raised among Saudis for Palestinians is intended for humanitarian purposes." Saudi foreign affairs advisor to Crown Prince Abdullah commented that the charge is "a ridiculous accusation," and that "no Saudi government money goes to Hamas, directly or indirectly."⁴⁶

⁴⁴ Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

⁴⁵ The New York Times, "Flow of Saudis' Cash to Hamas Scrutinized," September 17, 2003.

⁴⁶ The New York Times, "Flow of Saudis' Cash to Hamas Scrutinized," September 17, 2003.

Conclusions – Charities

Our review and analysis of Saudi Arabia’s charities sector as regards ML/FT offenses has identified some areas in which that system is fully or substantially compliant with relevant international standards. However, there are also several issues of concern, which will require continuing attention:

1. Administration

The charities charter provides for transparency regarding the management of charitable institutions in Saudi Arabia. However, there is a major gap stemming from the traditional organization of charities and the lack of accountability.

2. Financial Transparency

The Saudi Arabian regulation of charitable financial transparency provides for financial accounting transparency, lacks rigor regarding the external auditing of charities’ accounts and the interplay between charities and financial institutions.

3. Programmatic Verification

Saudi Arabian regulation does not provide a clear delineation of responsibilities regarding cooperation in the field of charities’ oversight and solicitation of the identities of the donors and the beneficiaries of charitable donations. While it seems the cooperation between the U.S. and Saudi Arabia is mainly focused on law enforcement, preventive action against the misuse of charities has not taken place, to date, in the kingdom.

4. Oversight Bodies

In theory, there appear to be many government agencies in charge of regulating and supervising charities. However, the specific role of each of these agencies is unclear and this situation results in both gaps and overlap of authority. The method for supervising international branches of Saudi charities requires additional attention.

5. Sanctions

Legal accountability and potential sanctions are an area lacking clarity. This interferes with efforts to create a deterrent effect.

International Cooperation

This chapter will examine the international cooperation component of Saudi Arabia's AML/CTF effort along three themes:

1. Ratification of International Conventions
2. Internal Actions Taken by the Kingdom of Saudi Arabia
3. Conclusion

It is vital in the fight to impede terrorist financing that the international community secures a high level of international intelligence cooperation and information, especially from countries that are key transit and source points of terrorist funds. One of the most important findings of the various commissions and groups investigating the financing of the 9/11 hijackers is that although traditional AML provisions are effective for tracking the unusual transaction patterns associated with money laundering, they are not sufficient for tracking the smaller and less distinguishable transactions associated with terror financing. In fact, no single 'terrorist financial profile' would have enabled either domestic or foreign law enforcement agencies to detect and block the funds transmitted to the 9/11 hijackers. In interviews, both law enforcement experts and compliance officers emphasized that the best way to track terror financing is to share lists of suspected perpetrators and pay close attention to their accounts. This process requires streamlined information sharing and intelligence cooperation between and among governments and private sectors on an international basis. This makes intelligence cooperation and information sharing with the Saudi intelligence agencies, Saudi financial institutions, and Saudi enforcement authorities integral to effectively combating terrorist financing.

Ratification of International Conventions

International conventions on money laundering and terrorist financing are the basis of international cooperation. They outline a common definition of the problem at hand and a common approach to solving it. Should a country not accede to such a convention, there is a danger that it will fall out of step with the international community and create a gap in the international CTF regime.

Any analysis of Saudi Arabia's level of international cooperation must thus begin with an examination of the conventions to which they have acceded. The ratification of the treaty itself does not necessarily indicate that appropriate actions are being taken within the Kingdom to address the issue of terrorist financing. At a minimum, however, treaties act as benchmark for evaluating KSA's level of international cooperation.

It is important to examine two issues in attempting to evaluate Saudi Arabia's compliance with international treaties:

- A. Is Saudi Arabia a signatory to the Vienna Convention, the Palermo Convention, and the United Nations International Convention for the Suppression of the Financing of Terrorism? Furthermore, is it a signatory to other important UN conventions pertaining to terrorism? If KSA is a signatory to these conventions, has it in fact ratified them?

Though the Vienna Convention and the Palermo Convention do not specifically address terrorist financing, they do address issues related to money laundering. And though, as mentioned in the introduction to this chapter, a good AML regime is not necessarily a good CTF regime, AML efforts are foundational to monitoring the flow of suspicious funds.

- B. Is Saudi Arabia implementing the international conventions cited above?

Principle 77: Compliance with International Money Laundering Treaties

Standard:

In accordance with FATF Recommendation 35¹⁰⁹, we have used the Vienna Convention and the Palermo Convention as the basis for assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective Saudi Arabia is in substantial compliance with this principle. This principle is not applicable to enforcement.

Law:

Saudi Arabia signed the Palermo Convention in December 2000, and has not ratified it.¹¹⁰ Saudi Arabia acceded to the Vienna Convention in January 1992.

We have thus not been able to verify Saudi Arabia's full compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's substantial compliance with the principle.

We have not seen any Saudi laws or regulations expressly implementing the terms of the Vienna Convention or the Palermo Convention. Articles 22-24 of the KSA-AMLL set forth guidelines for international cooperation.¹¹¹ Although these provisions are too vague to constitute effective implementation of the international cooperation components of the Vienna Convention or the Palermo Convention, they provide an encouraging legal basis for cooperation provisions in the forthcoming KSA-AMLL Implementation Rules.

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

While it is not difficult to evaluate Saudi Arabia's compliance with the issue of signing an international convention, the second part of the standard, which addresses implementation, is broad and far-reaching. In order to effectively evaluate compliance with this standard it is necessary to examine the key components of the various treaties. Collectively, they address the following major elements relevant to terror financing:

1. The criminalization of money laundering
2. The empowerment of law enforcement authorities to freeze and confiscate assets associated with money laundering

¹⁰⁹ FATF35: Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

¹¹⁰ Information on signature and ratification status is based on documents provided on the United Nations' website, at <<http://untreaty.un.org/English/TreatyEvent2003/index.htm>> (last visited on Nov. 13, 2003).

¹¹¹ Kingdom of Saudi Arabia, Regulations on Anti Money Laundering in KSA, Anti Money Laundering Law. August 2003, 6.

3. The obligation of regulatory authorities to establish a robust regulatory and supervisory regime for financial institutions
4. A smooth system of mutual legal assistance pertaining to AML and the encouragement of joint task forces and other methods of cooperation in addition to mutual legal assistance

A full evaluation of Saudi Arabia's compliance with these standards is outside the scope of this particular section, but is the subject of other parts of this report.

Principle 78: Ratification and Implementation of UN CFT Instruments

Standard:

In accordance with FATF Special Recommendation 1,¹¹² we have used the UN CFT Convention and the 2001 United Nations Security Council Resolution 1373 (“UNSC R1373”) as the basis for assessing Saudi Arabia’s compliance with this principle.

Assessment:

From a legal prospective Saudi Arabia is not in compliance with this principle. This principle is not applicable to enforcement.

Law:

Saudi Arabia signed the UN CFT Convention in November 2001, and has not ratified it.¹¹³ UNSC R1373, adopted under Chapter VII of the UN Charter, is automatically mandatory on Saudi Arabia with no further action necessary on the kingdom’s part. The offense of terrorist financing is set forth in the KSA-AMLL in Article 2(d).

We have not been able to verify Saudi Arabia’s compliance with this principle from a legal perspective. Our limited information tends to indicate that Saudi Arabia is non-compliant with the principle.

Saudi Arabia has failed to ratify the UN CFT Convention. We have not seen any laws or regulations expressly implementing the UN CFT Convention’s terms, or the UNSC R1373. As described under Principle 42, the language in Article 2(d) of the KSA-AMLL cannot be considered as sufficiently implementing those two international documents.

Further, we note that Saudi Arabia is not a signatory to the 1997 International Convention for the Suppression of Terrorist Bombings (the “UN CTB Convention”), despite being called upon by the UNSC R1373 to “[b]ecome [a party] as soon as possible to the relevant international conventions and protocols relating to terrorism” (Article 3(d)).

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

As discussed in Principle 35, the UN CTF is broad and far-reaching. The measures that Saudi Arabia has taken to implement some of the counter-terrorist financing measures described in it are discussed throughout this report.

¹¹² Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries should also immediately implement the United Nations resolutions relating to prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

¹¹³ Information on signature and ratification status is based on documents provided on the United Nations’ website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty11.asp> (last visited on Nov. 16, 2003).

Internal Actions Taken by KSA

As discussed in the introduction to this chapter, terrorist financing must be stopped through the exchange of information and assistance between and among governments and private institutions. That a country be a signatory of all the relevant conventions is important, but concrete measures must also be taken within its domestic regime. Most notably, Saudi Arabia's institutions must be authorized to share information with foreign authorities and empowered to take appropriate action to freeze and confiscate assets on the basis of international cooperation. Deficits in these areas could deny foreign authorities the information they need to track or prosecute terrorists or render fruitless foreign efforts to track finances to Saudi sources and transit points.

Principle 79: Authority for Prompt Response to Information-Sharing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia’s compliance with this principle. Specifically, in assessing the legal authority for responding to information-sharing requests by foreign countries, we have looked at Article 7 of the Vienna Convention, Article 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.¹¹⁴

Assessment:

We have been unable to verify Saudi Arabia’s compliance with this principle from either a legal or an enforcement perspective.

Law:

The KSA-AMLL, in Article 22, provides authority for sharing information with law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia’s compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia’s partial compliance with the principle.

Article 22 of the KSA-AMLL states that “Information disclosed by Financial and Non-Financial Institutions may be shared with concerned foreign authorities which are connected with the Kingdom through valid agreements or on the basis of reciprocity according to applicable legal procedures without prejudicing the confidentiality provisions and business practices of financial, non-financial and banking institutions.”

Without access to the Implementation Rules, the vague terms of Article 22 make it difficult to verify its level of compliance with this principle. However, we note with concern several aspects of Article 22 that suggest that Saudi Arabia’s compliance with this principle is partial at best:

a. Requirement of Mutuality.

The requirement in Article 22 of the KSA-AMLL that the concerned foreign authorities be “connected with the Kingdom through valid agreements or on the basis of reciprocity” appears to

¹¹⁴ FATF 36: Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

- a. Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.
- b. Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.
- c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
- d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts .

contradict the language of relevant international documents. Article 7(7) of the Vienna Convention expressly contemplates mutual legal assistance, including the provision of information, to foreign countries that “are not bound by a treaty of mutual legal assistance.” Article 7(15) of the same document lists permissible grounds for refusing mutual legal assistance; lack of a treaty or of reciprocity is not among them. Article 18(7) of the Palermo Convention, using similar language to Article 7(7) of the Vienna Convention, expressly provides for sharing of information with foreign countries that “are not bound by a treaty of mutual legal assistance.” Article 18(21) of the Palermo Convention, corresponding to Article 7(15) of the Vienna Convention, lists permissible grounds for refusing a request for mutual legal assistance; again, lack of a treaty or of reciprocity is not among them. Furthermore, we are unaware of any bilateral, multilateral or regional agreements that ‘connect’ “foreign authorities” to Saudi Arabia and provide for mutual sharing of reported information.

It remains to be seen how the Implementation Rules will interpret the reciprocity requirement, and to what extent the requirement will inhibit, in violation of the Vienna and Palermo Conventions, the rendering of mutual legal assistance to foreign countries.

b. *Limited Scope.*

Article 22 of the KSA-AMLL grants authority to share information discovered by “Financial and Non-Financial Institutions.” For a discussion of the limited scope of this term, and in particular its exclusion of the non-profit sector, see Principle 2b.

c. *Limited Range of Assistance.*

The KSA-AMLL grants authority to share “information” that has been “discovered.” It is unclear, pending publication of the Implementation Rules, whether this covers the provision of evidentiary items, expert evaluations, originals or certified copies of relevant documents and records, “including government, bank, financial, corporate or business records,” as contemplated by Article 18(3)(e)-(f) of the Palermo Convention. (Corresponding language appears in Article 7(2)(e)-(f) of the Vienna Convention.)

d. *Role of Bank Secrecy.*

The degree of international cooperation that the AMLL allows is further circumscribed by bank secrecy stipulations. Article 22, as quoted above, indicates that banks may not violate confidentiality provisions in cooperating with foreign authorities. Although we have not seen the Saudi bank secrecy regulations, we have no reason to believe that they make allowances for sharing confidential information with foreign authorities. The “confidentiality provisions” override is the most serious obstacle to compliance with this standard. It is noteworthy in this regard that the United Nations Convention against Transnational Organized Crime (the “Palermo Convention”), of which Saudi Arabia is a signatory and which is used by FATF as a benchmark for assessing AML compliance, declares that “States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy” (Article 18(8)).

e. *Legal Procedure*

We are unaware of any “applicable legal procedure” for effecting such information exchange. Perhaps this will be addressed in the Implementation Laws.

f. Designated Authority

The Palermo Convention requires States Parties to “designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution” (Article 8(13)). The KSA-AMLL does not designate a Saudi authority to which foreign authorities should address their requests for information. SAMA Regulations indicate that banks should cooperate with international parties through SAMA, but it is not clear that SAMA is the point of contact for foreign governments.¹¹⁵

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

Because intelligence collaboration and information sharing between governments and between financial bodies tends to be kept confidential, measuring Saudi implementation in this regard is extremely difficult. Our limited findings indicate that Saudi Arabia has taken steps since September 11, 2001 and the Riyadh bombings in May 2003 to cooperate more effectively with international enforcement agencies. One important sign of increased international cooperation has been the implementation of a Joint U.S.-Saudi Task Force devoted to the issue of terrorist financing. The joint task force was reportedly agreed to after a July 2003 phone call between President Bush and Saudi Crown Prince Abdullah.¹¹⁶ Apparently, the task force agreement was finalized during a visit of senior NSC, State, and Treasury officials to Saudi Arabia in August.¹¹⁷ This United States-Saudi CTF relationship has led to at least two specific cooperative initiatives. According to John Pistole, Assistant Director, counter-terrorism division, FBI, there has been significant cooperation between FBI and *the Mabahith* (Saudi Arabia’s internal intelligence agency).¹¹⁸ He testified that joint FBI-Mabahith operations are on-going. In addition, Saudi Arabia has established the joint task force with the FBI and IRS in Saudi Arabia since the May 12 2003 bombings in Saudi Arabia.¹¹⁹ Detailed information on these activities is unavailable and at this point it is too early to assess the joint task force’s work. Still, the existence of the task force and the FBI and IRS programs implies that some sort of understanding for information sharing exists between the United States and Saudi Arabia.

Too much should not be assumed about U.S.-Saudi cooperation, however. Matthew Levitt, a senior fellow at The Washington Institute for Near East Policy and a former FBI analyst specializing in terror financing, says that the joint task force is still experiencing problems in terms of cooperation.¹²⁰ Instead of being given access to a wide variety of sources and data, FBI agents must

¹¹⁵ SAMA AML-CTF Article 5.3

¹¹⁶ Farah, Douglas. *Washington Post*, <http://stacks.msnbc.com/news/957318.asp> (last visited on November 15, 2003).

¹¹⁷ Farah, Douglas. *Washington Post*, <http://stacks.msnbc.com/news/957318.asp> (last visited on November 15, 2003).

¹¹⁸ Pistole, John, testimony before the House committee on financial services, Sept. 24, 2003.

¹¹⁹ FBI Director Rober Mueller, June 2, 2003, “After the May 12 incidents in Riyadh, the US sent experts to the Kingdom for technical assistance.”

¹²⁰ Levitt, Matthew, Washington Institute for Near East Policy, interview, 11/12/03.

make very specific requests for information in order to obtain it.¹²¹ Unfortunately, successful law enforcement operations of this sort require access to a great deal of information; based on what investigators see, they can then pursue the proper specific details. Levitt believes that American law enforcement agents are not getting this necessary initial access.

We have two further reasons to be concerned that adequate information-sharing measures are not being implemented. First, Section 5.3 of SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing states that banks must conduct all of their international cooperation and information sharing through SAMA.¹²² This eliminates communication and cooperation between financial institutions on a transnational level. Interviews with former senior bankers at Saudi banks indicate that joint venture banks, which are partially owned by foreign firms, are not allowed to communicate information relevant to ML and TF to their parent companies without first going through SAMA.¹²³

Secondly, barriers to information-sharing likely extend beyond confidentiality regulations and other legal short-comings. The ingrained practice of not engaging in such sharing, which was attested to by senior banking executives with whom we spoke, might well prove resilient to legislation and enforcement, and create an independent obstacle to implementing effective international cooperation.¹²⁴

This study cannot definitively judge whether or not Saudi Arabia is cooperating on a satisfactory level with foreign authorities. This is due primarily to the fact that much of the information is classified and many members in the American government do not wish to speak about such a controversial issue. However, the information available indicates that while Saudi Arabia has made strides in increasing international cooperation, there is still much room for improvement.

¹²¹ Levitt, Matthew, Washington Institute for Near East Policy, interview, 11/12/03.

¹²² Rules Governing Anti Money Laundering and Combating Terrorist Financing, 12.

¹²³ Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.

¹²⁴ Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.

Principle 80: Authority for Prompt Response to Investigation-Assistance Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to investigation-assistance requests by foreign countries, we have looked at Article 7 of the Vienna Convention, Article 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.

Assessment:

From both a legal and enforcement perspective we have been unable to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL, in Article 23, provides authority for assisting investigations of law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's partial compliance with the principle.

Article 23 of the KSA-AMLL states that Saudi authorities, "upon a request from a concerned authority in a foreign country connected with the kingdom through ratified agreements or on the basis of reciprocity may order the pursuing of property, proceeds and instrumentalities connected with money laundering in accordance with Saudi applicable regulations."

Without access to the Implementation Rules, the vague terms of Article 23 make it difficult to verify its level of compliance with this principle. Our concerns with Article 23 echo those we have with Article 22 in Principle 36a; several aspects of Article 23 that suggest that Saudi Arabia's compliance with Principle 36b is partial at best:

a. *Requirement of Mutuality.*

See corresponding section in Principle 36a for discussion.

b. *Limited Range of Assistance.*

The KSA-AMLL grants authority to "pursue" assets on behalf of foreign authorities. It is unclear, pending publication of the Implementation Rules, whether this authority extends to taking evidence or statements from persons, effecting service of judicial documents, executing searches and seizures, examining objects and sites, and facilitating the voluntary appearance of persons in the requesting State Party, as contemplated by Article 18(3) of the Palermo Convention. (Corresponding language appears in Article 7(2) of the Vienna Convention.)

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

See corresponding section in Principle 36a for discussion

Principle 81: Authority for Prompt Response to Asset-Freezing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia’s compliance with this principle. Specifically, in assessing the legal authority for responding to asset-freezing requests by foreign countries, we have looked at Articles 5 and 7 of the Vienna Convention, Articles 12, 13 and 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.¹²⁵

Assessment:

We have not been able to verify Saudi Arabia’s compliance with this principle from either a legal or an enforcement perspective.

Law:

The KSA-AMLL, in Article 23, provides authority for freezing assets based on requests by law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia’s compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia’s partial compliance with the principle.

Article 23 of the KSA-AMLL states that Saudi courts may, “pursuant to a request by a court or concerned authority in a foreign country connected with the kingdom through ratified agreements or on the basis of reciprocity, order the impounding of property, proceeds or instrumentalities connected with money laundering in accordance with Saudi applicable regulations.”

Our concerns with Article 23 in regard to this principle are similar to those concerns discussed in Principle 36a and 36b. Without access to the Implementation Rules, the vague terms of Article 23 make it difficult to verify its level of compliance with this principle. Several aspects of Article 23 that suggest that Saudi Arabia’s compliance with Principle 38a is partial at best:

a. *Requirement of Mutuality.*

See corresponding section in Principle 36a for discussion.

b. *Limited Range of Assistance.*

The KSA-AMLL grants authority to “impound” assets pursuant to requests by foreign authorities. It is unclear, pending publication of the Implementation Rules, whether this authority covers taking “measures to identify, trace and freeze or seize” the assets as contemplated by Article

¹²⁵ FATF38: There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

13(2) of the Palermo Convention. (Corresponding language appears in Article 5(4)(b) of the Vienna Convention.)

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

Very little information is available in this regard. A document released by the Saudi embassy in Washington states that “Saudi Arabia on September 26, 2001 required Saudi banks to identify and freeze all assets relating to terrorist suspects and entities per the list issued by the US government on September 23, 2001,” it is unknown whether this action was taken or how many assets were frozen.¹²⁶ Saudi Arabia has claimed to seize terrorist assets but it is unknown whether these seizures were the result of coordination with other countries.

The government of Saudi Arabia has also released information on two related cases. In March of 2002, Saudi and the United States jointly blocked the accounts of the Bosnia and Somalia branches of Al-Haramain Islamic Foundation. In September 2002, US Treasury and Saudi government took joint action, freezing the assets of the Rabita Trust, and those of its director Wa’el Hamza Julaidan, an associate of Osama bin Laden.¹²⁷ It is known that both these cases were based on US information and requests for enforcement.

In addition, Saudi Arabia has stated that a special committee was established, drawing from the Ministry of Interior, Ministry of Foreign Affairs, the Intelligence Agency and SAMA, to deal with requests from international bodies and countries with regard to combating terrorist financing.¹²⁸ However, there is no information available on this committee.

In regard to implementation, we would like information on the following questions:

- 1) With which governments does Saudi Arabia have a reciprocal agreement to cooperate on AML-CTF matters?
- 2) How many requests have foreign governments submitted to Saudi Arabia for action on specific CTF cases?
- 3) How has Saudi Arabia responded to these requests?
- 4) What is the process by which assets are seized in Saudi Arabia?
- 5) What happens to assets seized in Saudi Arabia as the result of an international investigation?

¹²⁶ A document released by Saudi Embassy in the US, “Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism,” p. 6.

¹²⁷ A document released by Saudi Embassy in the US, “Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism,” p.2

¹²⁸ A document released by Saudi Embassy in the US, “Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism,” p.2

Principle 82: Authority for Prompt Response to Confiscation Judgment-Executing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to confiscation requests by foreign countries, we have looked at Article 5 of the Vienna Convention, and Articles 12 and 13 of the Palermo Convention.

Assessment:

From a legal perspective we have found Saudi Arabia to be partially compliant with this principle. From an enforcement perspective we have been unable to determine Saudi Arabia's compliance.

Law:

The KSA-AMLL, in Article 24, provides authority for confiscating assets based on rulings by courts of foreign countries.

We have found Saudi Arabia to be partially compliant with this principle from a legal perspective.

Article 24 of the KSA-AMLL states that rulings by foreign courts "providing for the confiscation of property, proceeds or instrumentalities connected with money laundering, issued by a competent court in a foreign country connected with the kingdom through a valid agreement or convention, or on the basis of reciprocity, may be recognized by the kingdom if the property, proceeds or instrumentalities covered by the court ruling are subject to confiscation under Saudi applicable law."

We do not consider the Article 24 language to be only partially with this principle for the following reasons:

a. Requirement of Mutuality.

The requirement in Article 24 of the KSA-AMLL that the concerned foreign authorities be "connected with the Kingdom through a valid agreement or convention, or on the basis of reciprocity" appears to contradict the language of relevant international documents. Article 5(4)(a) of the Vienna Convention requires a Party in whose territory confiscable assets are situated, upon receiving a request from "another Party having jurisdiction over [a relevant] offence," to submit the requesting Party's order of confiscation to the requested Party's "competent authorities, with a view to giving it effect to the extent requested." No limits are imposed on the requesting Party's identity other than its having jurisdiction over the relevant offense. The Palermo Convention contains corresponding language in its Article 13(1).

By imposing a requirement that the requesting Party be connected to the Kingdom, Article 24 of the KSA-AMLL appears to constrain its grant of authority to respond to asset-confiscation rulings by foreign courts, in a manner inconsistent with international documents.

b. *Hortatory Language.*

The KSA-AMLL indicates that rulings by foreign courts “may” be recognized by the kingdom. This contrasts unfavorably with the language of the Vienna Convention, which provides in Article 5(4)(a) that a requested Party “shall” submit the order of confiscation to its competent authorities with a view to giving effect to it. The Palermo Convention contains corresponding language in its Article 13(1).

c. *Limits of Saudi confiscatory powers.*

The language in Article 24 of the KSA-AMLL conditions the confiscation of assets upon such assets’ being subject to confiscation under Saudi applicable law. For a discussion of the limits of Saudi applicable law, see Principle 3.

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

See corresponding section in Principle 38a for discussion

Principle 83: Extradition for ML and FT

Standard:

We have used FATF recommendation 39¹²⁹ in assessing Saudi Arabia's compliance with this principle.

Assessment

From a legal perspective we have found that Saudi Arabia we are not able to verify Saudi Arabia's compliance with this principle. From enforcement perspective we are not be able to verify Saudi Arabia's compliance with the principle.

Law:

There are no laws and procedures that specifically address the extradition of individuals charged with a ML or FT.

AML Articles 22-24, on the basis of reciprocity, deal broadly with international cooperation. However, they address information sharing and asset tracking and seizure only; no mention is made of the fate of the perpetrators.

While it would to desirable to see specific mention of extradition made in Saudi AML-CTF laws, it must be noted that Saudi Arabia is not bound to extradite for offense that it undertakes to prosecute itself. See the Criminal Law chapter for an analysis of Saudi Arabia's ability to try individuals for FT.

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

We are not aware of any efforts on the part of a foreign government to extradite an individual charged with ML or FT from Saudi Arabia.

¹²⁹ Countries should recognize money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings

Conclusions – International Cooperation

In evaluating Saudi Arabia's level of international cooperation we have found the following outstanding issues.

1. Ratification of Treaties

Saudi Arabia has yet to ratify the Palermo Convention on international crime or the UN CFT Convention. These two documents embody the international consensus on combating money laundering and terrorist financing. The fact that Saudi Arabia has not ratified them raises the concern that the Kingdom does not see the challenge at hand or its solution in the same way as much of the rest of the international community. A disagreement on either of these points is likely to hinder the necessary cooperative effort.

It is also of concern that Saudi Arabia has neither signed nor ratified the 1997 UN Convention on Terror Bombing. Any disagreement on what constitutes an act of terrorism could impede international efforts to gain Saudi cooperation to track and prosecute individuals that the Kingdom does not consider terrorists.

2. Vagueness of the Laws

Article 22-24 of the new AML laws outline requirements pertaining to international cooperation. However, these laws are vague, and we hope that additional requirements will be included in the new implementation laws pertaining to the AML law.

3. Role of Banking Secrecy

Saudi Arabia has several laws that could impede international cooperation, most particularly Article 22 of the KSA-AMLL. Although we have not seen the Saudi bank secrecy regulations, we have no reason to believe that they make allowances for sharing confidential information with foreign authorities.

4. Law Enforcement Cooperation

We have very little information on Saudi cooperation with foreign law enforcement agencies, but there is some indication that U.S. authorities are not getting the cooperation they need from their Saudi counterparts.

Annex 1

The Forty Recommendations (2003)

LEGAL SYSTEMS

Scope of the criminal offence of money laundering

Recommendation 1

Countries should criminalise money laundering on the basis of [the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances \(the Vienna Convention\)](#) and [the 2000 United Nations Convention on Transnational Organized Crime \(the Palermo Convention\)](#).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the [designated categories of offences](#) [3].

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

Footnotes:

[3] See the definition of "designated categories of offences" in the Glossary.

Recommendation 2

Countries should ensure that:

- a. The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.
- b. Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisional measures and confiscation

Recommendation 3

Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Recommendation 4

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

Customer due diligence and record-keeping

Recommendation 5

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

- a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information [\[4\]](#).
- b. Identifying the [beneficial owner](#), and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.
- c. Obtaining information on the purpose and intended nature of the business relationship.
- d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times. **(See Interpretative Notes: [Recommendation 5](#) and [Recommendations 5, 12 and 16](#)) /**

Footnotes:

[4] Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

Recommendation 6

Financial institutions should, in relation to [politically exposed persons](#), in addition to performing normal due diligence measures:

- a. Have appropriate risk management systems to determine whether the customer is a politically exposed person.
- b. Obtain senior management approval for establishing business relationships with such customers.
- c. Take reasonable measures to establish the source of wealth and source of funds.
- d. Conduct enhanced ongoing monitoring of the business relationship.

(See Interpretative Note)

Recommendation 7

Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

- a. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
- b. Assess the respondent institution's anti-money laundering and terrorist financing controls.
- c. Obtain approval from senior management before establishing new correspondent relationships.
- d. Document the respective responsibilities of each institution.
- e. With respect to "[payable-through accounts](#)", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts

of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

Recommendation 8

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

Recommendation 9

Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

- a. A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- b. The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations. ([See Interpretative Note](#))

Recommendation 10

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority. ([See Interpretative Note](#))

Recommendation 11

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. ([See Interpretative Note](#))

Recommendation 12

The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to [designated non-financial businesses and professions](#) in the following situations:

- a. Casinos – when customers engage in financial transactions equal to or above the applicable [designated threshold](#).

- b. Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.
- c. Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- d. Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:
 - buying and selling of real estate;
 - managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organisation of contributions for the creation, operation or management of companies;
 - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
- e. Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

[\(See Interpretative Note\)](#)

Reporting of suspicious transactions and compliance

Recommendation 13

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

Recommendation 14

Financial institutions, their directors, officers and employees should be:

- a. Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the [FIU](#), even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
- b. Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

[\(See Interpretative Note\)](#)

Recommendation 15

Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

- a. The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
- b. An ongoing employee training programme.
- c. An audit function to test the system.

[\(See Interpretative Note\)](#)

Recommendation 16

The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

- a. Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
- b. Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- c. Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. **(See Interpretative Notes: [Recommendation 16](#) and [Recommendations 5, 12, and 16](#))**

Other measures to deter money laundering and terrorist financing

Recommendation 17

Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

Recommendation 18

Countries should not approve the establishment or accept the continued operation of [shell banks](#). Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

Recommendation 19

Countries should consider:

- a. Implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.
- b. The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

Recommendation 20

Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

Recommendation 21

Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

Recommendation 22

Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

Recommendation 23

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

For financial institutions subject to the [Core Principles](#), the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing. ([See Interpretative Note](#))

Recommendation 24

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

- a. Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:
 - casinos should be licensed;
 - competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino

- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.
- b. Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

Recommendation 25

The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions. ([See Interpretative Note](#))

INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

Recommendation 26

Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of [STR](#) and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR. ([See Interpretative Note](#))

Recommendation 27

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries. ([See Interpretative Note](#))

Recommendation 28

When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

Recommendation 29

[Supervisors](#) should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

Recommendation 30

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

Recommendation 31

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

Recommendation 32

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

Transparency of legal persons and arrangements

Recommendation 33

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

Recommendation 34

Countries should take measures to prevent the unlawful use of [legal arrangements](#) by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

INTERNATIONAL CO-OPERATION

Recommendation 35

Countries should take immediate steps to become party to and implement fully [the Vienna Convention](#), [the Palermo Convention](#), and [the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism](#). Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual legal assistance and extradition

Recommendation 36

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

- a. Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

- b. Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.
- c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
- d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Recommendation 37

Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Recommendation 38

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets. ([See Interpretative Note](#))

Recommendation 39

Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

Recommendation 40

Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

- a. Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.
- b. Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.
- c. Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection. ([See Interpretative Note](#))

GLOSSARY

In these Recommendations the following abbreviations and references are used:

“Beneficial owner” refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

“Core Principles” refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

“Designated categories of offences” means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;

- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

“Designated non-financial businesses and professions” means:

- a. Casinos (which also includes internet casinos).
- b. Real estate agents.
- c. Dealers in precious metals.
- d. Dealers in precious stones.
- e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
 - acting as a formation agent of legal persons;
 - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
 - providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
 - acting as (or arranging for another person to act as) a trustee of an express trust;
 - acting as (or arranging for another person to act as) a nominee shareholder for another person.

“Designated threshold” refers to the amount set out in the Interpretative Notes.

“Financial institutions” means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[\[5\]](#)
2. Lending.[\[6\]](#)
3. Financial leasing.[\[7\]](#)
4. The transfer of money or value.[\[8\]](#)

5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
 - a. money market instruments (cheques, bills, CDs, derivatives etc.);
 - b. foreign exchange;
 - c. exchange, interest rate and index instruments;
 - d. transferable securities;
 - e. commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.^[9]
13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

Footnotes:

- [5] This also captures private banking.
- [6] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).
- [7] This does not extend to financial leasing arrangements in relation to consumer products.
- [8] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.
- [9] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

“**FIU**” means financial intelligence unit.

“**Legal arrangements**” refers to express trusts or other similar legal arrangements.

“**Legal persons**” refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

“**Payable-through accounts**” refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

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

“Shell bank” means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

“STR” refers to suspicious transaction reports.

“Supervisors” refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

“the FATF Recommendations” refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

Annex 2

FATF Special Recommendations on Terrorist Financing

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts. For further information on the Special Recommendations as related to the self-assessment process, see the [Guidance Notes](#).

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations. ([See Interpretative Note](#)) ([See Best Practices Paper](#))

IV. Reporting suspicious transactions related to terrorism

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

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions. [\(See Interpretative Note\)](#) [\(See Best Practices Paper\)](#)

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number). [\(See Interpretative Note\)](#)

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

- i. by terrorist organisations posing as legitimate entities;
- ii. to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
- iii. to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

Annex 3

Basel Committee on Banking Supervision

Customer due diligence for banks

October 2001

Working Group on Cross-border Banking

Co-Chairs:

Mr Charles Freeland, Deputy Secretary General, Basel Committee on Banking Supervision

Mr Colin Powell, Chairman, Offshore Group of Banking Supervisors, and Chairman, Jersey Financial Services Commission

Bermuda Monetary Authority Mr D Munro Sutherland

Cayman Islands Monetary Authority Mr John Bourbon
Mrs Anna McLean

Banque de France/Commission Bancaire Mr Laurent Ettori

Federal Banking Supervisory Office of Germany Mr Jochen Sanio
Mr Peter Kruschel

Guernsey Financial Services Commission Mr Peter G Crook (until April 2001)
Mr Philip Marr (since April 2001)

Banca d'Italia Mr Giuseppe Godano

Financial Services Agency, Japan Mr Kiyotaka Sasaki (until July 2001)
Mr Hisashi Ono (since July 2001)

Commission de Surveillance du Secteur Financier,
Luxembourg
Mr Romain Strock

Monetary Authority of Singapore Mrs Foo-Yap Siew Hong
Ms Teo Lay Har

Swiss Federal Banking Commission Mr Daniel Zuberbühler
Ms Dina Balleyguier

Financial Services Authority, United Kingdom Mr Richard Chalmers

Board of Governors of the Federal Reserve System Mr William Ryback

Federal Reserve Bank of New York Ms Nancy Bercovici

Office of the Comptroller of the Currency Mr Jose Tuya
Ms Tanya Smith

Secretariat Mr Andrew Khoo

Table of Contents

I. Introduction.....	2
II. Importance of KYC standards for supervisors and banks.....	3
III. Essential elements of KYC standards	5
1. Customer acceptance policy	6
2. Customer identification.....	6
2.1 General identification requirements.....	7
2.2 Specific identification issues	8
2.2.1 Trust, nominee and fiduciary accounts.....	8
2.2.2 Corporate vehicles.....	8
2.2.3 Introduced business.....	9
2.2.4 Client accounts opened by professional intermediaries.....	9
2.2.5 Politically exposed persons.....	10
2.2.6 Non-face-to-face customers.....	11
2.2.7 Correspondent banking.....	12
3. On-going monitoring of accounts and transactions.....	13
4. Risk management	14
IV. The role of supervisors.....	14
V. Implementation of KYC standards in a cross-border context	15
Annex 1: Excerpts from <i>Core Principles Methodology</i>	18
Annex 2: Excerpts from FATF recommendations	20

Customer due diligence for banks

I. Introduction

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

2. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking¹³⁰ to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued as a consultative document in January 2001. Following a review of the comments received, the Working Group has revised the paper and the Basel Committee is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes. It is important to acknowledge that supervisory practices of some jurisdictions already meet or exceed the objective of this paper and, as a result, they may not need to implement any changes.

3. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).¹³¹ It is not the Committee's intention to duplicate the efforts of the FATF. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems. The Basel Committee and the Offshore Group of Banking Supervisors (OGBS) continue to support strongly the adoption and implementation of the FATF recommendations, particularly those relating to banks, and intend the standards in this paper to be consistent with the FATF recommendations. The Committee and the OGBS will also consider the adoption of any higher standards introduced by the FATF as a result of its current review of the 40 Recommendations. Consequently, the Working Group has been and will remain in close contact with the FATF as it develops its thoughts.

4. The Basel Committee's approach to KYC is from a wider prudential, not just anti money laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their

¹³⁰ This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

¹³¹ The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 29 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations, Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

6. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.

7. The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all non-bank financial institutions and professional intermediaries of financial services such as lawyers and accountants.

II. Importance of KYC standards for supervisors and banks

8. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's 40 Recommendations on combating money-laundering¹³² have international recognition and application. It is not the intention of this paper to duplicate that work.

9. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

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

10. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially **reputational, operational, legal and concentration risks**. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

11. **Reputational risk** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect

¹³² See FATF recommendations 10 to 19 which are reproduced in Annex 2

themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

12. **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

13. **Legal risk** is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practise due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

14. Supervisory concern about **concentration risk** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

15. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analysing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

16. Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

17. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct¹³³ issued by industry organisations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to banks on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

III. Essential elements of KYC standards

¹³³ An example of an industry code is the "Global anti-money-laundering guidelines for Private Banking" (also called the Wolfsberg Principles) that was drawn up in October 2000 by twelve major banks with significant involvement in private banking.

18. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 *Core Principles Methodology* further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 1 sets out the relevant extracts from the *Core Principles* and the *Methodology*.)

19. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements"¹³⁴. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

1. Customer acceptance policy

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level.

2. Customer identification

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

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);

¹³⁴ *Core Principles Methodology*, Essential Criterion 1

- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

22. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

23. Banks should “document and enforce policies for identification of customers and those acting on their behalf”.¹³⁵ The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

24. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records¹³⁶. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.

However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

26. Banks should develop “clear standards on what records must be kept on customer identification and individual transactions and their retention period”¹³⁷. Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer’s on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. As the starting point and natural follow-up of the identification process, banks should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

2.1 General identification requirements

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encouraged to provide guidance to assist

¹³⁵ *Core Principles Methodology*, Essential Criterion 2.

¹³⁶ The application of new KYC standards to existing accounts is currently subject to FATF review.

¹³⁷ *Core Principles Methodology*, Essential Criterion 2.

banks in designing their own identification procedures. The Working Group intends to develop essential elements of customer identification requirements.

28. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, the bank should close the account and return the monies to the source from which they were received¹³⁸

29. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

30. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered¹³⁹ accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

2.2 Specific identification issues

31. There are a number of more detailed issues relating to customer identification which need to be addressed. Several of these are currently under consideration by the FATF as part of a general review of its 40 recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts

32. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries¹⁴⁰.

2.2.2 Corporate vehicles

33. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies, may make proper identification of customers or beneficial owners

¹³⁸ Subject to any national legislation concerning handling of suspicious transactions.

¹³⁹ In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

¹⁴⁰ Beneficiaries should be identified as far as possible when defined. It is recognised that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children and some may be conditional on the occurrence of specific events. In addition, beneficiaries being specific classes of individuals (e.g. employee pension funds) may be appropriately dealt with as pooled accounts as referred to in paragraphs 38-9.

difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

34. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies needs to be obtained. In the case of entities which have a significant proportion of capital in the form of bearer shares, extra vigilance is called for. A bank may be completely unaware that the bearer shares have changed hands. The onus is on banks to put in place satisfactory procedures to monitor the identity of material beneficial owners. This may require the bank to immobilise the shares, e.g. by holding the bearer shares in custody.

2.2.3 Introduced business

35. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

36. The Basel Committee recommends that banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:¹⁴¹

- it must comply with the minimum customer due diligence practices identified in this paper;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

2.2.4 Client accounts opened by professional intermediaries

¹⁴¹ The FATF is currently engaged in a review of the appropriateness of eligible introducers.

37. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

38. Banks often hold “pooled” accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are “sub-accounts” which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

39. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank. National supervisory guidance should clearly set out those circumstances in which banks need not look beyond the intermediary. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 36 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

40. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers¹⁴² bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this paper or to the requirements of comprehensive anti-money laundering legislation, then the bank should not permit the intermediary to open an account.

2.2.5 Politically exposed persons

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons (“PEPs”) are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

42. Accepting and managing funds from corrupt PEPs will severely damage the bank’s own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

43. Some countries have recently amended or are in the process of amending their laws

¹⁴² The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients.

and regulations to criminalise active corruption of foreign civil servants and public officers in accordance with the relevant international convention.¹⁴³ In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

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

2.2.6 Non-face-to-face customers

45. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of nonface- to-face customer identification is being discussed by the FATF, and is also under review in the context of amending the 1991 EEC Directive.

46. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.¹⁴⁴¹⁵

47. Even though the same documentation can be provided by face-to-face and nonface-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult.

48. In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for nonface-to-face customers as for those available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

¹⁴³ See OECD Convention on *Combating Bribery of Foreign Public Officials in International Business Transactions*, adopted by the Negotiating Conference on 21 November 1997.

¹⁵ The Electronic Banking Group of the Basel Committee issued a paper on risk management principles for electronic banking in May 2001.

Examples of measures to mitigate risk include:

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

2.2.7 Correspondent banking

49. Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

50. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country.

Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

51. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being “noncooperative” in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts.

52. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 36.

3. On-going monitoring of accounts and transactions

53. On-going monitoring is an essential aspect of effective KYC procedures. Banks can

only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-money laundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.

Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.¹⁴⁵ As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

4. Risk management

55. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively and are, at a minimum, in accordance with local supervisory practice.

¹⁴⁵ It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that PEPs (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel. There should also be internal procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and and/or supervisory authorities.

56. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

57. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are well versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

58. All banks must have an ongoing employee-training programme so that bank staff are adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

59. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. The role of supervisors

60. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

61. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

62. Supervisors have a duty not only to ensure their banks maintain high KYC standards

to protect their own safety and soundness but also to protect the integrity of their national banking system.¹⁴⁶ Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

V. Implementation of KYC standards in a cross-border context

63. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis. This is a challenging task for banks and supervisors alike.

64. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

65. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

66. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

67. Criminal elements are likely to be drawn toward jurisdictions with such impediments.

¹⁴⁶ Many supervisors also have a duty to report any suspicious, unusual or illegal transactions that they detect, for example, during onsite examinations.

Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

68. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation¹⁴⁷ to facilitate information sharing between the two supervisors would be helpful in this regard.

69. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the banks' general policies and procedures for customer due diligence and for dealing with suspicions.

¹⁴⁷ See the Basel Committee paper *Essential elements of a statement of cooperation between banking supervisors* (May 2001).

Excerpts from *Core Principles Methodology*

Principle 15: Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict “know-your-customer” rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.

Essential criteria

1. The supervisor determines that banks have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. This includes the prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities.
2. The supervisor determines that banks have documented and enforced policies for identification of customers and those acting on their behalf as part of their antimoney-laundering program. There are clear rules on what records must be kept on customer identification and individual transactions and the retention period.
3. The supervisor determines that banks have formal procedures to recognise potentially suspicious transactions. These might include additional authorisation for large cash (or similar) deposits or withdrawals and special procedures for unusual transactions.
4. The supervisor determines that banks appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local statutory and regulatory anti-money laundering requirements.
5. The supervisor determines that banks have clear procedures, communicated to all personnel, for staff to report suspicious transactions to the dedicated senior officer responsible for anti-money laundering compliance.
6. The supervisor determines that banks have established lines of communication both to management and to an internal security (guardian) function for reporting problems.
7. In addition to reporting to the appropriate criminal authorities, banks report to the supervisor suspicious activities and incidents of fraud material to the safety, soundness or reputation of the bank.
8. Laws, regulations and/or banks' policies ensure that a member of staff who reports suspicious transactions in good faith to the dedicated senior officer, internal security function, or directly to the relevant authority cannot be held liable.
9. The supervisor periodically checks that banks' money laundering controls and their systems for preventing, identifying and reporting fraud are sufficient. The supervisor has adequate enforcement powers (regulatory and/or criminal prosecution) to take action against a bank that does not comply with its anti-money laundering obligations.
10. The supervisor is able, directly or indirectly, to share with domestic and foreign

financial sector supervisory authorities information related to suspected or actual criminal activities.

11. The supervisor determines that banks have a policy statement on ethics and professional behaviour that is clearly communicated to all staff.

Additional criteria

1. The laws and/or regulations embody international sound practices, such as compliance with the relevant forty Financial Action Task Force Recommendations issued in 1990 (revised 1996).

2. The supervisor determines that bank staff is adequately trained on money laundering detection and prevention.

3. The supervisor has the legal obligation to inform the relevant criminal authorities of any suspicious transactions.

4. The supervisor is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.

5. If not performed by another agency, the supervisor has in-house resources with specialist expertise on financial fraud and anti-money laundering obligations.

Annex 4

COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS

International Best Practices

Introduction and definition

1. The misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source. This issue has captured the attention of the Financial Action Task Force (FATF), the G7, and the United Nations, as well as national authorities in many regions. Within the FATF, this has rightly become the priority focus of work to implement Special Recommendation VIII (Non-profit organisations).
2. Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, foundations, fundraising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.
3. This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations **that engage in raising or disbursing funds** for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works” from being misused or exploited by the financiers of terrorism.

Statement of the Problem

4. Unfortunately, numerous instances have come to light in which the mechanism of charitable fundraising – *i.e.*, the collection of resources from donors and its redistribution for charitable purposes– has been used to provide a cover for the financing of terror. In certain cases, the organisation itself was a mere sham that existed simply to funnel money to terrorists. However, often the abuse of nonprofit organisations occurred without the knowledge of donors, or even of members of the management and staff of the organisation itself, due to malfeasance by employees and/or managers diverting funding on their own. Besides financial support, some non-profit organisations have also provided cover and logistical support for the movement of terrorists and illicit arms. Some examples of these kinds of activities were presented in the 2001-2002 FATF Report on Money Laundering Typologies¹⁴⁸; others are presented in the annex to this paper.

Principles

5. The following principles guide the establishment of these best practices:
 - The charitable sector is a vital component of the world economy and of many national economies and social systems that complements the activity of the governmental and business sectors in supplying a broad spectrum of public services and improving quality of life. We wish to safeguard and maintain the practice of charitable giving and the strong and diversified community of institutions through which it operates.
 - Oversight of non-profit organisations is a co-operative undertaking among government, the charitable community, persons who support charity, and those whom it serves. Robust oversight mechanisms

¹⁴⁸ Published February 2002 and available at http://www.fatf-gafi.org/FATDocs_en.htm#Trends.

and a degree of institutional tension between non-profit organisations and government entities charged with their oversight do not preclude shared goals and complementary functions – both seek to promote transparency and accountability and, more broadly, common social welfare and security goals.

- Government oversight should be flexible, effective, and proportional to the risk of abuse. Mechanisms that reduce the compliance burden without creating loopholes for terrorist financiers should be given due consideration. Small organisations that do not raise significant amounts of money from public sources, and locally based associations or organisations whose primary function is to redistribute resources among members may not necessarily require enhanced government oversight.
- Different jurisdictions approach the regulation of non-profit organisations from different constitutional, legal, regulatory, and institutional frameworks, and any international standards or range of models must allow for such differences, while adhering to the goals of establishing transparency and accountability in the ways in which non-profit organisations collect and transmit funds. It is understood as well that jurisdictions may be restricted in their ability to regulate religious activity.
- Jurisdictions may differ on the scope of purposes and activities that are within the definition of “charity,” but all should agree that it does not include activities that directly or indirectly support terrorism, including actions that could serve to induce or compensate for participation in terrorist acts.
- The non-profit sector in many jurisdictions has representational, self-regulatory, watchdog, and accreditation organisations that can and should play a role in the protection of the sector against abuse, in the context of a public-private partnership. Measures to strengthen self-regulation should be encouraged as a significant method of decreasing the risk of misuse by terrorist groups.

Areas of focus

6. Preliminary analysis of the investigations, blocking actions, and law-enforcement activities of various jurisdictions indicate several ways in which non-profit organisations have been misused by terrorists and suggests areas in which preventive measures should be considered.

(i) Financial transparency

7. Non-profit organisations collect hundreds of billions of dollars annually from donors and distribute those monies – after paying for their own administrative costs – to beneficiaries. Transparency is in the interest of the donors, organisations, and authorities. However, the sheer volume of transactions conducted by non-profit organisations combined with the desire not to unduly burden legitimate organisations generally underscore the importance of risk and size-based proportionality in setting the appropriate level of rules and oversight in this area.

a. Financial accounting

- Non-profit organisations should maintain and be able to present full program budgets that account for all programme expenses. These budgets should indicate the identity of recipients and how the money is to be used. The administrative budget should also be protected from diversion through similar oversight, reporting, and safeguards.
- Independent auditing is a widely recognised method of ensuring that that accounts of an organisation accurately reflect the reality of its finances and should be considered a best practice. Many major non-profit organisations undergo audits to retain donor confidence, and regulatory authorities in some jurisdictions require them for non-profit organisations. Where practical, such audits should be conducted to ensure that such organisations are not being abused by terrorist groups. It should be

noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.

b. Bank accounts:

- It is considered a best practice for non-profit organisations that handle funds to maintain registered bank accounts, keep its funds in them, and utilise formal or registered financial channels for transferring funds, especially overseas. Where feasible, therefore, non-profit organisations that handle large amounts of money should use formal financial systems to conduct their financial transactions. Adoption of this best practice would bring the accounts of non-profit organisations, by and large, within the formal banking system and under the relevant controls or regulations of that system.

(ii) Programmatic verification

8. The need to verify adequately the activities of a non-profit organisation is critical. In several instances, programmes that were reported to the home office were not being implemented as represented. The funds were in fact being diverted to terrorist organisations. Non-profit organizations should be in a position to know and to verify that funds have been spent as advertised and planned.

a. Solicitations

9. Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organisation should then ensure that such funds are used for the purpose stated.

b. Oversight

10. To help ensure that funds are reaching the intended beneficiary, non-profit organizations should ask following general questions:

- Have projects actually been carried out?
- Are the beneficiaries real?
- Have the intended beneficiaries received the funds that were sent for them?
- Are all funds, assets, and premises accounted for?

c. Field examinations

11. In several instances, financial accounting and auditing might be insufficient protection against the abuse of non-profit organisations. Direct field audits of programmes may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists. Given considerations of risk-based proportionality, across-the-board examination of all programmes would not be required. However, non-profit organisations should track programme accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted.

d. Foreign operations

12. When the home office of the non-profit organisation is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages. Where possible, a non-profit organisation should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.

(iii) Administration

13. Non-profit organisations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.

14. Much has been written about the responsibilities of Boards of Directors in the corporate world and recent years have seen an increased focus and scrutiny of the important role of the Directors in the healthy and ethical functioning of the corporation. Directors of non-profit organisations, or those with equivalent responsibility for the direction and control of an organisation's management, likewise have a responsibility to act with due diligence and a concern that the organisation operates ethically. The directors or those exercising ultimate control over a non-profit organisation need to know who is acting in the organisation's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organisations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.

15. Directors should act with diligence and probity in carrying out their duties. Lack of knowledge or passive involvement in the organisation's affairs does not absolve a director – or one who controls the activities or budget of a non-profit organisation – of responsibility. To this end, directors have responsibilities to:

- The organisation and its members to ensure the financial health of the organisation and that it focuses on its stated mandate.
- Those with whom the organisation interacts, like donors, clients, suppliers.
- All levels of government that in any way regulate the organisation.

16. These responsibilities take on new meaning in light of the potential abuse of non-for-profit organisations for terrorist financing. If a non-profit organisation has a board of directors, the board of directors should:

- Be able to identify positively each board and executive member;
- Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings;
- Formalise the manner in which elections to the board are conducted as well as the manner in which a director can be removed;
- Ensure that there is an annual independent review of the finances and accounts of the

organisation;

- Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organisations;
- Ensure an appropriate balance between spending on direct programme delivery and administration;
- Ensure that procedures are put in place to prevent the use of the organisation's facilities or assets to support or condone terrorist activities.

Oversight bodies

17. Various bodies in different jurisdictions interact with the charitable community. In general, preventing misuse of non-profit organisations or fundraising organisations by terrorists has not been a historical focus of their work. Rather, the thrust of oversight, regulation, and accreditation to date has been maintaining donor confidence through combating waste and fraud, as well as ensuring that government tax relief benefits, where applicable, go to appropriate organisations. While much of this oversight focus is fairly easily transferable to the fight against terrorist finance, this will also require a broadening of focus.

18. There is not a single correct approach to ensuring appropriate transparency within non-profit organisations, and different jurisdictions use different methods to achieve this end. In some, independent charity commissions have an oversight role, in other jurisdictions government ministries are directly involved, just to take two examples. Tax authorities play a role in some jurisdictions, but not in others. Other authorities that have roles to play in the fight against terrorist finance include law enforcement agencies and bank regulators. Far from all the bodies are governmental – private sector watchdog or accreditation organisations play an important role in many jurisdictions.

(i) Government Law Enforcement and Security officials

19. Non-profit organisations funding terrorism are operating illegally, just like any other illicit financier; therefore, much of the fight against the abuse of non-profit organisations will continue to rely heavily on law enforcement and security officials. Non-profit organisations are not exempt from the criminal laws that apply to individuals or business enterprises.

- Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organisations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organisations.

(ii) Specialised Government Regulatory Bodies

20. A brief overview of the pattern of specialised government regulation of non-profit organisations shows a great variety of practice. In England and Wales, such regulation is housed in a special Charities Commission. In the United States, any specialised government regulation occurs at the sub-national (state) level. GCC member countries oversee non-profit organisations with a variety of regulatory bodies, including government ministerial and intergovernmental agencies.

- In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organisations. Specifically, terrorist financing experts should work with non-profit organization oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.

(iii) Government Bank, Tax, and Financial Regulatory Authorities

21. While bank regulators are not usually engaged in the oversight of non-profit organisations, the earlier discussion of the importance of requiring charitable fund-raising and transfer of funds to go through formal or

registered channels underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules, etc – in the fight against terrorist abuse or exploitation of non-profit organisations.

22. In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.

- Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organisations by terrorist groups or supporters is shared as appropriate.

(iv) Private Sector Watchdog Organisations

23. In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organisations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organisations by terrorists. Not only do they contain observers knowledgeable of fundraising organisations, they are also very directly interested in preserving the legitimacy and reputation of the non-profit organisations. More than any other class of participants, they have long been engaged in the development and promulgation of “best practices” for these organisations in a wide array of functions.

24. Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organisations in their attempt to put best practices into place for combating the misuse of non-profit organisations. Such engagement could include a dialogue on how to improve such practices.

Sanctions

25. Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.

TYOLOGIES OF TERRORIST MISUSE OF NON-PROFIT ORGANISATIONS

Annex

Example 1: Non-profit front organisation

1. In 1996, a number of individuals known to belong to the religious extremist groups established in the south-east of an FATF country (Country A) convinced wealthy foreign nationals, living for unspecified reasons in Country A, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group. It was later established that “S”, a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above.

2. This place of worship intended for the local community in fact also served as a place to lodge clandestine “travellers” from extremist circles and collect funds. For example, soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a “foundation” would be more suitable for collecting and using large funds without attracting the attention of local authorities. A foundation was thus reportedly established for this purpose.

3. It is also believed that part of “S’s” activities in heading a multipurpose international financial network (for which investments allegedly stood at USD 53 million for Country A in 1999 alone) was to provide support to a terrorist network. “S” had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country A, was allegedly a platform for collecting funds. “S” also purchased several buildings in the south of Country A with the potential collusion of a notary and a financial institution.

4. When the authorities of Country A blocked a property transaction on the basis of the foreign investment regulations, the financial institution’s director stepped in to support his client’s transaction and the notary presented a purchase document for the building thus ensuring that the relevant authorisation was delivered. The funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction to conceal their origin when they were used in Country A.

5. Even though a formal link has not as yet been established between the more or less legal activities of the parties in Country A and abroad and the financing of terrorist activities carried out under the authority of a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

Example 2: Fraudulent solicitation of donations

6. One non-profit organisation solicited donations from local charities in a donor region, in addition to fund raising efforts conducted at its headquarters in a beneficiary region. This non-profit organisation falsely asserted that the funds collected were destined for orphans and widows. In fact, the finance chief of this organisation served as the head of organised fundraising for Usama bin Laden. Rather than providing support for orphans and widows, funds collected by the non-profit organisation were turned over to al-Qaida operatives.

Example 3: Branch offices defraud headquarters

7. The office director for a non-profit organisation in a beneficiary region defrauded donors from a donor region to fund terrorism. In order to obtain additional funds from the headquarters, the branch office

pped the number of orphans it claimed to care for by providing names of orphans that did not exist or who had died. Funds then sent for the purpose of caring for the non-existent or dead orphans were instead diverted to al-Qaida terrorists.

8. In addition, the branch office in a beneficiary region of another non-profit organisation based in a donor region provided a means of funnelling money to a known local terrorist organisation by disguising funds as intended to be used for orphanage projects or the construction of schools and houses of worship. The office also employed members of the terrorist organisations and facilitated their travel.

Example 4: Aid worker's Misuse of Position

9. An employee working for an aid organisation in a war-ravaged region used his employment to support the ongoing activities of a known terrorist organisation from another region. While working for the aid organisation as a monitor for work funded in that region, the employee secretly made contact with weapons smugglers in the region. He used his position as cover as he brokered the purchase and export of weapons to the terrorist organisation.

Annex 5

1981 Regulations Regarding Associations and Charitable Institutions

- I. STEPS NECESSARY TO OPEN A CHARITY
 - a. 20 or more individuals are necessary to open a charity.
 - b. All members must have no criminal record.
 - c. Permission is required from Ministry of Labor and Social Affairs (MLSA)
 - d. Charities must register with the MLSA.
 - e. Once a charity receives authorization from MLSA, the board of directors of the charity must make an official announcement in the government circular.
 - f. A charity must announce the names of the board of directors, the organization chart and the goals of organization.

- II. DEFINITION OF CHARITY

Provides social services in money or kind, for education and health without gaining financial profit. Charities are forbidden from making money.

- III. SUBSIDIARY INFO
 - a. Charities cannot open subsidiaries without the permission of MLSA.
 - b. Changes in organization chart should be forwarded to MLSA for authorization.

- IV. THE MLSA LICENSES CHARITIES
 - a. The license contains date of registration
 - b. The license give each charity an identification number.
 - c. The date the registration was announced in the official record.
 - d. The license includes the address of charity.

- V. ORGANIZATION CHART SHOULD INCLUDE THE FOLLOWING:
 - a. The name of the charity, official address and jurisdiction.
 - b. The goals of the charity.
 - c. The name, age, personal address of the founding members.
 - d. Requirements necessary for membership.
 - e. Budget and allocations of finances.
 - f. The fiscal operating year.
 - g. Internal financial controls.
 - h. Information about subsidiaries, their missions and goals the necessary requirements to be a subsidiary. Rules of termination of partnership with subsidiaries and parent.
 - i. Conditions and rules to change or amend the organization,
 - j. Rules for dissolving of charity and outcome of remaining proceeds.
 - k. Proceeds after dissolving charity must go to another registered charity.

- VI MISCELLANEOUS

- VII. DEFINITION OF PUBLIC ASSOCIATION
 - a. An association must be in existence for one year with all of its members having paid their dues prior to being considered an association.
 - b. The public association must hold all its meeting in its official address except with prior approval from MLSA. The rules, invitation, agenda and procedures of the meeting must be published in advanced.
 - c. MLSA must be notified 15 days prior to meeting with copy of the agenda.

- VIII. SELECTION OF BOARD OF DIRECTORS
 - a. Election must be done by secret ballot, with a MLSA representative present at the election.

- b. Board of directors have 4 years term limits.
- c. 90 days prior to election the MLSA must receive a list of candidates, if after 60 days the association has not heard anything from the MLSA then this implies approval of candidate. The MLSA representative can nullify the results of the election due to cause up to 15 days after the election.
- d. Within 10 days of every meeting the minutes must be sent to MLSA, the MLSA has 20 days to block the actions detailed in the minutes.
- e. By-laws for meetings must be established.

IX. THE INTERIM BOARD OF DIRECTORS.

MLSA can appoint an interim board of directors if the MLSA thinks it serves in the best interest of the association.

- X. The board of directors must submit all financial statements to the MLSA and an operating budget and pro-forma budget signed by president or vice president, treasurer, accountant, an auditing firm, and secretary general of the organization.

XI. THE ASSOCIATION RULES

- a. Associations must keep records of all correspondence.
- b. Files must contain name, address, age, date of membership, occupation, and the amount of dues made for all members.
- c. Minutes of all the meetings must be kept at headquarters.
- d. Must keep a record of all financial statements, budgets, and money raised, its sources and how it is spent.
- e. The association must have registered legal council.
- f. The finances of the association must be kept at banks within the KSA, and withdrawals must have signatures from two members in the association. These two must be recognized as those enabled to withdraw funds in the association bylaws and organizational chart.
- g. The association must put its name, identification number and jurisdiction in all files, correspondences and printouts.

XII. SUBSIDIES AND DONATIONS

- a. The MLSA provides the association with statutory subsidies.
- b. Charities are able to raise funds and accept donations, and accept will bequests, in the condition that such bequests are in accordance with the laws of the kingdom.

- XIII. The MLSA can set up management contracts with charities to enable them to use its offices and pay the MLSA to run its offices.

XIV. NULLIFICATION OF ASSOCIATIONS

Members of association can decide to nullify it according to rules contain on its organizational chart.

XV. THE MLSA CAN DECIDE TO NULLIFY ASSOCIATIONS UNDER THE FOLLOWING CONDITIONS:

- a. If the number of members of the association drops below 20.
- b. If the association is not respecting its goals or commits fraud or crimes.
- c. If the association is not able to meet its financial commitments.
- d. If the association transgresses its organizational chart.
- e. Fails to respect commonly accepted cultural behavior.
- f. The MLSA can appoint a new board of directors to associations.

XVI. ASSOCIATION FINANCES

- a. Association members responsible for managing association finances cannot use those funds for personal use.

- b. The MLSA provides the rules for association liquidation and will decide who will receive liquidated assets in case it is not clearly stated in the charity's charter.

XVII. MLSA JURISDICTION

- a. The MLSA is the official organization in charge of supervising the activities of charities and the implementation of its plans. They have the right to review all files and registers. If an MLSA officer presents himself and requests information about the association, the association must provide this officer with such information.
- b. The MLSA has the authority to block any decision emanating from the association that is in opposition to the organizational chart.

XVIII. GENERAL CABINET FOR THE CIVILIAN SERVICE

The MLSA and the General Cabinet for the Civilian Service are in charge of providing certificates and authorization to any citizen who uses any cultural, educational or other type of service provided by charities.

XIX. CREATION OF THE INSTITUTION AND ITS GOALS

It is possible to create a charitable institution for a non-pecuniary goal with the condition that this institution profits only its members or pre-defined groups.

XX. The MLSA has a special file listing all charitable institutions.

XXI. The charitable institution acquires its legal status once registered in this file.

XXII. The same rules organizing charities are applicable to a charitable organization.

XXIII. Charitable institutions cannot receive subsidies from the MLSA nor can they accept small donations (tabarra), but they can still accept large donations (hibet) and receive bequests.

XXIV. After the liquidation of any charitable institution, its money goes to a charitable association according to the directives of the MLSA unless the institutions organizational chart states that proceeds shall go to a specific charitable activity.

XXV. These regulations apply to charitable associations and charitable institutions irregardless of whether they registered or were established prior to the publication of these rules. These regulations do not apply to special charitable institutions created by Royal decree.

XXVI. These regulations emanate from the MLSA and should be announced in the official bulletin.

XXVII. These regulations supercede any conflicting regulations.

XXVIII. These regulations come into effect 60 days after announcement in the official bulletin.

