Financial Action Task Force

Groupe d'action financière

RBA GUIDANCE FOR ACCOUNTANTS

17 June 2008

TABLE OF CONTENTS

SECTION ONE: USING THE GUIDANCE - PURPOSE OF THE RISK-BASED APPROACH.....1

Chapter One: Background and Context.....1
Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges.....4
Chapter Three: FATF and the Risk-Based Approach.....7

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES.....12

Chapter One: High-level Principles for Creating a Risk-Based Approach.....12
Chapter Two: Implementation of the Risk-Based Approach.....15

SECTION THREE: GUIDANCE FOR ACCOUNTANTS ON IMPLEMENTING A RISK-BASED APPROACH.....21

Chapter One: Risk Categories.....21
Chapter Two: Application of a Risk-based Approach.....25
Chapter Three: Internal Controls.....28

ANNEXES.....30

ANNEX 1 – SOURCES OF FURTHER INFORMATION.....30

A. Financial Action Task Force documents.....30
B. Other sources of information to help assist countries' and accountants' risk assessment of countries and cross-border activities.....30

ANNEX 2 – GLOSSARY OF TERMINOLOGY.....32

ANNEX 3 – MEMBERS OF THE ELECTRONIC ADVISORY GROUP.....34

GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

HIGH LEVEL PRINCIPLES AND PROCEDURES FOR ACCOUNTANTS

SECTION ONE: USING THE GUIDANCE

PURPOSE OF THE RISK-BASED APPROACH

Chapter One: Background and Context

1. In June 2007 the FATF adopted Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures, which includes guidance for public authorities and guidance for financial institutions. This was the culmination of extensive consultation between private and public sector members of an Electronic Advisory Group (EAG) established by the FATF.

2. In addition to financial institutions, the FATF Recommendations also cover a number of designated non-financial businesses and professions (DNFBPs). At its June 2007 meeting, the FATF's Working Group on Evaluations and Implementation (WGEI) endorsed a proposal to convene a meeting of representatives from the DNFBPs to assess the possibility of developing guidance on the risk-based approach for their sectors, using the same structure and style as the completed guidance for financial institutions.

3. This meeting was held in September 2007 and was attended by representatives of organisations which represent lawyers, notaries, trust and company service providers, accountants, casinos, real estate agents, and dealers in precious metals and dealers in precious stones. This private sector group expressed an interest in contributing to FATF guidance on implementing a risk-based approach for their sectors. The guidance for the DNFBPs would follow the principles of the risk-based approach already established by FATF, and would highlight risk factors specific to the DNFBPs, as well as suggest mitigation strategies that fit with the particular activities and businesses of the DNFBPs. The FATF established another EAG to facilitate the work.

4. The private sector group met again in December 2007 and was joined by a number of specialist public sector members. Separate working groups comprising public and private sectors members were established, and private sector chairs were appointed.

5. The EAG continued work until this guidance for accountants was presented to the WGEI. After further international consultation with both public and private sectors, the FATF adopted this guidance at its June 2008 Plenary. Guidance for each of the other DNFBP sectors is being published separately.

Purpose of the guidance

6. The purpose of this guidance is to:

- Support the development of a common understanding of what the risk-based approach involves.
- Outline the high-level principles involved in applying the risk-based approach.
- Indicate good practice in the design and implementation of an effective risk-based approach.

7. However it should be noted that applying a risk-based approach is not mandatory. A properly applied risk-based approach does not necessarily mean a reduced burden, although it should result in a more cost effective use of resources. For some countries, applying a rules-based system might be more appropriate. Countries will need to make their own determinations on whether to apply a risk-based approach, based on their specific ML/FT risks, size and nature of the DNFBP activities, and other relevant information. The issue of timing is also relevant for countries that may have applied anti-money laundering/combating the financing of terrorism (AML/CFT) measures to DNFBPs, but where it is uncertain whether the DNFBPs have sufficient experience to implement and apply an effective risk-based approach.

Target audience, status and content of the guidance

8. This guidance has been prepared for, and in relation to, accountants in public practice[1]. The roles and therefore risks of the different DNFBP sectors are usually separate. However, in some business areas, there are inter-relationships between different DNFBP sectors, and between the DNFBPs and financial institutions. For example, accountants may be instructed by businesses or professionals within other DNFBP sectors or by financial institutions. Accountants may also undertake trust and company services covered by the FATF Recommendations. For such activities, accountants should make reference to the guidance on the risk-based approach for Trust and Company Service Providers (TCSPs).

9. DNFBPs provide a range of services and activities that vastly differ, *e.g.* in their methods of delivery and in the depth and duration of the relationships formed with clients, and the size of their operation. This Guidance is written at a high level to cater for the differing practices of accountants in different countries, and the different levels and forms of supervision or monitoring that may apply. Each country and its national authorities should aim to establish a partnership with its accountants and other DNFBP sectors that will be mutually beneficial to combating money laundering and terrorist financing.

10. The primary target audience of this guidance is the accountants themselves, when they conduct activities which fall within the ambit of the FATF Recommendations, as described below.

11. Recommendation 12 mandates that the requirements for customer due diligence, record-keeping, and paying attention to all complex, unusual large transactions set out in Recommendation 5, 6, and 8 to 11 apply to DNFBPs in certain circumstances. Specifically, Recommendation 12 applies to accountants when they prepare for or carry out transactions for their client concerning the following activities:

- Buying and selling of real estate;
- Management 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.

[1] 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.

- Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

12. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions (see paragraphs 129 to 132) and internal AML/CFT controls, and Recommendation 21 regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, apply to accountants when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in R.12 above.

13. Where accountants are subject to obligations of professional secrecy or legal professional privilege (similar in nature to that of legal professionals), they 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 under the laws of that country. Professional secrecy/legal professional privilege are not the same as client confidentiality.

14. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, they are also not required to report suspicious transactions.

15. The wider audience for this guidance includes countries, designated competent authorities, and self-regulatory organisations (SROs), which are considering how to apply AML/CFT measures to accountants. Countries need to identify the most appropriate regime, tailored to address individual country risks, which takes into consideration the idiosyncrasies and activities of accountants and other DNFBP sectors in their country. This regime should recognise the differences between the DNFBP sectors, as well as the differences between the DNFBPs and financial institutions. However, this guidance does not override the purview of national authorities.

<u>Observation on the particular activities carried out by accountants</u>

16. The following general observation about accountants should help inform the approach. Consideration should also be given to the particular activities performed by accountants on a national basis.

17. This Guidance is addressed to accountants in public practice, on applying a risk-based approach to compliance with those of FATF's Recommendations that apply to them. It 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**.** Accountants in business are referred to professional or other alternative sources of Guidance, on the appropriate action to take in relation to suspected illegal activity by their employer or a third party.

18. Accountants in practice may provide a very wide range of services, to a very diverse range of clients. For example, services may include (but are not restricted to):

- Audit and assurance services.
- Book-keeping and the preparation of annual and periodic accounts.
- Tax compliance work, and advice on the legitimate minimisation of tax burdens.
- Internal audit, and advice on internal control and risk minimisation.

- Regulatory and compliance services, including outsourced regulatory examinations and remediation services.
- Insolvency/receiver-managers/bankruptcy related services.
- Advice on the structuring of transactions, and succession advice.
- Advice on investments and custody of client money.
- Forensic accountancy.

19. In many countries, accountants are the first professional consulted by many small businesses and individuals when seeking general business advice and a wide range of regulatory and compliance advice. Where services are not within their competence, accountants advise on an appropriate source of further assistance[2]. Accountants typically refer to those benefiting from their services as "clients" rather than "customers", and so that term has generally been used throughout this paper.

20. Some of the functions performed by accountants that are the most useful to the potential launderer include:

a. Financial and tax advice – Criminals with a large amount of money to invest may pose as individuals hoping to minimise their tax liabilities or desiring to place assets out of reach in order to avoid future liabilities.

b. Creation of corporate vehicles or other complex legal arrangements (trusts, for example) – such structures may serve to confuse or disguise the links between the proceeds of a crime and the perpetrator.

c. Buying or selling of property – Property transfers serve as either the cover for transfers of illegal funds (layering stage) or else they represent the final investment of these proceeds after their having passed through the laundering process (integration stage).

d. Performing financial transactions – Sometimes accountants may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.).

e. Gaining introductions to financial institutions.

Chapter Two: The Risk-Based Approach – Purpose, Benefits and Challenges

The purpose of the risk-based approach

21. The FATF Recommendations contain language that permits countries, to the degree specified, to adopt a risk-based approach to combating money laundering and terrorist financing. That language also authorises countries to permit DNFBPs to use a risk-based approach in applying certain of their AML/CFT obligations.

22. By adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk. This can inadvertently lead to a "tick box" approach with the

[2] The European Federation of Accountants (FEE) has issued a study on market access across the Member States of the European Union, which gives an indication of the types of services provided by accountants, and the ways in which they can vary between countries.

focus on meeting regulatory requirements rather than on combating money laundering or terrorist financing efficiently and effectively.

23. A number of the DNFBP sectors, including accountants in countries where accountancy is a regulated profession, are already subject to regulatory or professional requirements which complement AML/CFT measures. Where possible, it will be beneficial for accountants to devise their AML/CFT policies and procedures in a way that harmonises with other regulatory or professional requirements. A risk-based AML/CFT regime should help ensure that honest clients can access the services provided by accountants, but creates barriers to those who seek to misuse those services.

24. A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. Countries will need to identify the main vulnerabilities and address them accordingly. Accountants will need this assistance to help them to identify higher risk customers, products and services, delivery channels, and geographical locations. These are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve.

25. The strategies to manage and mitigate the identified money laundering and terrorist financing activities are typically aimed at preventing the activity from occurring through a mixture of deterrence (*e.g.* appropriate CDD measures), detection (*e.g.* monitoring and suspicious transaction reporting), and record-keeping (*e.g.* to facilitate investigations).

26. Proportionate procedures should be designed based on assessed risk. Higher risk areas should be subject to enhanced procedures; this would include measures such as enhanced customer due diligence checks and enhanced transaction monitoring. It also follows that in instances where risks are low, simplified or reduced controls may be applied. (See also paragraph 118 on variables that affect risk).

27. There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, an effective risk-based approach does involve identifying and categorising money laundering and terrorist financing risks, and establishing reasonable controls based on risks identified.

28. An effective risk-based approach will allow accountants to exercise reasonable business and professional judgement with respect to clients. Application of a reasoned and well-articulated risk-based approach will justify the judgements made with regard to managing potential money laundering and terrorist financing risks. A risk-based approach should not be designed to prohibit accountants from continuing with legitimate business or from finding innovative ways to diversify their business.

29. Regardless of the strength and effectiveness of AML/CFT controls, criminals will continue to attempt to move illicit funds undetected and will, from time to time, succeed. They may be more likely to target DNFBP sectors if other routes become more difficult. For this reason, DNFBPs, including accountants, may be more or less vulnerable depending on the effectiveness of the AML/CFT procedures applied in other sectors. A risk-based approach allows DNFBPs, including accountants, to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

30. A reasonably designed and effectively implemented risk-based approach will provide an appropriate and effective control structure to manage identifiable money laundering and terrorist financing risks. However, it must be recognised that any reasonably applied controls, including controls implemented as a result of a reasonably designed and effectively implemented risk-based approach will not identify and detect all instances of money laundering or terrorist financing. Therefore, designated competent authorities, SROs, law enforcement, and judicial authorities must take into account and give due consideration to a well reasoned risk-based approach. In cases where there is a failure to implement an adequately designed risk-based approach or failure of a risk-based

programme that was not adequate in its design, regulators, SROs, law enforcement or judicial authorities should take action as necessary and appropriate.

Potential benefits and challenges of the risk-based approach

Benefits

31. The adoption of a risk-based approach to combating money laundering and terrorist financing can yield benefits for all parties including the public. Applied effectively, the approach should allow a more efficient and effective use of resources and minimise burdens on clients. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively.

32. For accountants, the risk-based approach allows the flexibility to approach AML/CFT obligations using specialist skills and responsibilities. This requires accountants to take a wide and objective view of their activities and clients.

33. Efforts to combat money laundering and terrorist financing should also be flexible in order to adapt as risks evolve. As such, accountants will use their judgement, knowledge and expertise to develop an appropriate risk-based approach for their particular organisation, structure and business activities.

Challenges

34. A risk-based approach is not necessarily an easy option, and there may be challenges when implementing the necessary measures. Some challenges may be inherent to the use of the risk-based approach. Others may stem from the difficulties in making the transition to a risk-based system, A number of challenges, however, can also be seen as offering opportunities to implement a more effective system. The challenge of implementing a risk-based approach with respect to terrorist financing is discussed in more detail at paragraphs 46-50 below.

35. The risk-based approach is challenging to both public and private sector entities. Such an approach requires resources and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems and to train personnel. It further requires that sound and well-trained judgement be exercised in the design and implementation of procedures and systems. It will certainly lead to a greater diversity in practice which should lead to innovations and improved compliance. However, it may also cause uncertainty regarding expectations, difficulty in applying uniform regulatory treatment, and an increased lack of understanding by clients regarding information required.

36. Implementing a risk-based approach requires that accountants have a sound understanding of the risks and are able to exercise sound judgement. This requires the building of expertise including for example, through training, recruitment, taking professional advice and “learning by doing”. The process will always benefit from information sharing by designated competent authorities and SROs. The provision of good practice guidance is also valuable. Attempting to pursue a risk-based approach without sufficient expertise may lead to flawed judgements. Accountants may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, thereby creating vulnerabilities.

37. Accountants may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. This may also be true at various levels of management of accounting firms. However, in situations where management fails to recognise or underestimates the risks, a culture may develop that allows for inadequate resources to be devoted to compliance, leading to potentially significant compliance failures.

38. Designated competent authorities and SROs should place greater emphasis on whether accountants have an effective decision-making process with respect to risk management, and sample testing should be used or individual decisions reviewed as a means to test the effectiveness of an accountant's overall risk management. Designated competent authorities and SROs should recognise that even though appropriate risk management structures and procedures are regularly updated, and the relevant policies, procedures, and processes are followed, decisions may still be made that are incorrect in light of additional information not reasonably available at the time.

39. A risk-based approach requires an accountant to exercise professional judgement. This will result in diversity of practice and detail between firms, although both may meet legislative requirements. Such diversity of practice will require that designated competent authorities and SROs make greater effort to identify and disseminate guidelines on good practice, and may pose challenges to staff working to monitor compliance. The existence of good practice guidance, training, industry studies and other available information and materials will assist the designated competent authorities and SROs in determining whether an accountant has made sound risk-based judgements.

40. Recommendation 25 requires adequate feedback to be provided to the financial sector and DNFBPs. Such feedback helps institutions and businesses to more accurately assess the money laundering and terrorist financing risks and to adjust their risk programmes accordingly. This in turn makes the detection of suspicious activity more likely and improves the quality of suspicious transaction reports. As well as being an essential input to any assessment of country or sector wide risks, the promptness and content of such feedback is relevant to implementing an effective risk-based approach.

The potential benefits and potential challenges can be summarised as follows:

Potential Benefits:

- Better management of risks
- Efficient use and allocation of resources
- Focus on real and identified threats
- Flexibility to adapt to risks that change over time

Potential Challenges:

- Identifying appropriate information to conduct a sound risk analysis
- Addressing short term transitional costs
- Greater need for more expert staff capable of making sound judgements.
- Developing appropriate regulatory response to potential diversity of practice.

Chapter Three: FATF and the Risk-Based Approach

41. The varying degrees of risk of money laundering or terrorist financing for particular types of DNFBPs, including accountants, or for particular types of customers/clients, or transactions is an important consideration underlying the FATF Recommendations. According to the Recommendations, with regard to DNFBPs there are specific Recommendations where the degree of risk is an issue that a country either must take into account (if there is higher risk), or may take into account (if there is lower risk)**.**

Specific risk references

42. The risk-based approach is either incorporated into the Recommendations (and the Methodology) in specific and limited ways in a number of Recommendations, or it is inherently part of or linked to those Recommendations. For instance, for DNFBPs, including accountants, risk is addressed in three principal areas (a) Customer Due Diligence (*R.5, 6, 8 and 9*); (b) businesses'

internal control systems (*R.15*); and (c) the approach of oversight/ monitoring of DNFBPs, including accountants (*R.24*).

Customer Due Diligence (R. 5, 6, 8 and 9)

43. Risk is referred to in several forms:

a) Higher risk – Under Recommendation 5, a country must require its DNFBPs, including accountants, to perform enhanced due diligence for higher-risk customers, business relationships or transactions. Recommendation 6 (politically exposed persons) is an example of this principle, detailing a higher risk scenario requiring enhanced CDD.

b) Lower risk – A country may also permit its DNFBPs, including the accountants, to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). Accountants may thus reduce or simplify (but not avoid completely) the required measures.

c) Risk arising from innovation – Under Recommendation 8, a country must require its DNFBPs, including accountants, to give special attention to the risks arising from new or developing technologies that might favour anonymity.

d) Risk assessment mechanism – The FATF standards expect that there will be an adequate mechanism by which designated competent authorities and SROs assess or review the procedures adopted by accountants to determine the degree of risk and how they manage that risk, as well as to review the actual determinations themselves. This expectation applies to all areas where the risk-based approach is applied. In addition, where the designated competent authorities and SROs have issued guidelines on a suitable approach to risk-based procedures, it will be important to establish that these have been followed. The Recommendations also recognise that country risk is a necessary component of any risk assessment mechanism (R.5 & 9).

Internal Control Systems (R.15)

44. Under Recommendation 15, the development of "appropriate" internal policies, training and audit systems will need to include a specific, and ongoing, consideration of the potential money laundering and terrorist financing risks associated with clients, products and services, geographic areas of operation and so forth. The Interpretative Note to Recommendation 15 makes it clear that a country may allow DNFBPs, including the accountants, to have regards to money laundering and terrorist financing risks and to the size of the business when determining the type and extent of measures required.

Regulation and Oversight by Designated Competent Authorities or SROs (R.24)

45. Countries should ensure that accountants are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining whether the system for monitoring and ensuring compliance is appropriate, regard may be had to the risk of money laundering or terrorist financing in a given business, *i.e.* if there is a proven low risk then lesser monitoring measures may be taken.

<u>Applicability of the risk-based approach to terrorist financing</u>

46. There are both similarities and differences in the application of a risk-based approach to terrorist financing and money laundering. They both require a process for identifying and assessing risk. However, the characteristics of terrorist financing makes its detection more difficult and the implementation of mitigation strategies challenging, due to considerations such as the relatively low

value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

47. Funds that are used to finance terrorist activities may be derived either from criminal activity or may be from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing, though the activity, which may be indicative of suspicion, may not be identified as or connected to terrorist financing. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services to further their goals, with the only covert fact being the intended use of such materials and services purchased. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering. However in all cases, it is not the responsibility of the accountants to determine the type of underlying criminal activity, or intended terrorist purpose, rather the accountant's role is to identify and report the suspicious activity. The FIU and law enforcement authorities will then examine the matter further and determine if there is a link to terrorist financing.

48. The ability of accountants to detect and identify potential terrorist financing transactions, without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities, is significantly more challenging than is the case for potential money laundering and other suspicious activity. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering).

49. Particular individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which sanctions apply and the obligations on accountants to comply with those sanctions are decided by individual countries and are not a function of risk. Accountants may commit a criminal offence if they undertake business with a listed individual, organisation or country, or its agent, in contravention of applicable sanctions.

50. For these reasons, this Guidance has not comprehensively addressed the application of a risk-based approach to terrorist financing. It is clearly preferable that a risk-based approach be applied where reasonably practicable, but further consultation with key stakeholders is required to identify a more comprehensive set of indicators of the methods and techniques used for terrorist financing, which can then be factored into strategies to assess terrorist financing risks and devise measures to mitigate them. DNFBPs, including the accountants, would then have an additional basis upon which to more fully develop and implement a risk-based process for terrorist financing.

Limitations to the risk-based approach

51. There are circumstances in which the application of a risk-based approach will not apply, or may be limited. There are also circumstances in which the application of a risk-based approach may not apply to the initial stages of a requirement or process, but then will apply to subsequent stages. The limitations to the risk-based approach are usually the result of legal or regulatory requirements that mandate certain actions to be taken.

52. Requirements to freeze assets of identified individuals or entities, in countries where such requirements exist, are independent of any risk assessment. The requirement to freeze is absolute and

cannot be impacted by a risk-based process. Similarly, while the identification of potential suspicious transactions can be advanced by a risk-based approach, the reporting of suspicious transactions, once identified, is not risk-based (see paragraphs 130-134).

53. There are several components to customer due diligence – Identification and verification of identity of customers and beneficial owners, obtaining information on the purposes and intended nature of the business relationships, and conducting ongoing due diligence. Of these components, the identification and verification of identity of customers are requirements which must be completed regardless of the risk-based approach. However, in relation to all the other CDD components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep records and documents that have been obtained for due diligence purposes, as well as transaction records, is not dependent on risk levels.

54. Countries may allow accountants to apply reduced or simplified measures where the risk of money laundering or terrorist financing is lower. However, these reduced or simplified measures do not necessarily apply to all aspects of CDD. Moreover, where these exemptions are subject to certain conditions being met, it is necessary to verify that these conditions apply, and where the exemption applies under a certain threshold, measures should be in place to prevent transactions from being split artificially to avoid the threshold. In addition, information beyond client identity, such as client location, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a client should be sufficient to determine whether to go further, and in many cases client monitoring will provide additional information.

55. Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk clients, monitoring is needed to verify that transactions match the initial low risk profile and if not, trigger a process for appropriately revising the client's risk rating. Equally, risks for some clients may only become evident once a relationship with a client has begun. This makes appropriate and reasonable monitoring of client transactions an essential component of a properly designed risk-based approach. However within this context it should be understood that not all transactions, accounts or clients will be monitored in exactly the same way. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this could be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption.

Distinguishing risk-based monitoring and risk-based policies and processes

56. Risk-based policies and processes should be distinguished from risk-based supervision/monitoring by designated competent authorities or SROs. There is a general recognition within supervisory/monitoring field that resources should be allocated taking into account the risks posed by individual firms or businesses. The methodology adopted by the designated competent authorities or SROs to determine allocation of monitoring resources should cover the business focus, the risk profile and the internal control environment, and should permit relevant comparisons between firms or businesses. The methodology used for determining the allocation of resources will need updating on an ongoing basis so as to reflect the nature, importance and scope of the risks to which individual firms or businesses are exposed. Consequently, this prioritisation should lead designated competent authorities or SROs to focus increased regulatory attention on firms or businesses that engage in activities assessed to present a higher risk of money laundering or terrorist financing.

57. However, it should also be noted that the risk factors taken into account to prioritise the designated competent authorities' or SROs' work will depend not only on the intrinsic risk associated with the activity undertaken, but also on the quality and effectiveness of the risk management systems put in place to address such risks.

58. Since designated competent authorities or SROs should have already assessed the quality of risk management controls throughout the accounting sector, it is reasonable that their assessments of these controls be used, at least in part, to inform money laundering and terrorist financing risk assessments conducted by individual firms or businesses.

Summary box: A risk-based approach to countering money laundering and terrorist financing at the national level: key elements for success

- Accountants, designated competent authorities and SROs should have access to sufficiently detailed, reliable and actionable information about the threats, and how to implement a risk-based approach.
- There must be emphasis on cooperative arrangements among the policy makers, law enforcement, regulators, and the private sector.
- Authorities should publicly recognise that the risk-based approach will not eradicate all elements of risk.
- Authorities have a responsibility to establish an atmosphere in which accountants need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Regulators' and SROs' supervisory staff must be well-trained in the risk-based approach, both as applied by supervisors/SRO and by the accountants.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

Chapter One: High-level Principles for Creating a Risk-Based Approach

59. The application of a risk-based approach to countering money laundering and the financing of terrorism will allow designated competent authorities and SROs, including oversight boards, and accountants to use their resources most effectively. This chapter sets out five high-level principles that should be considered by countries when designing a risk-based approach. They could be considered as setting out a broad framework of good practice.

60. The five principles set out in this paper are intended to assist countries in their efforts to improve their AML/CFT regimes. They are not intended to be prescriptive, and should be applied in a manner that is well-considered and appropriate to the particular circumstances of the country in question.

Principle one: Understanding and responding to threats and vulnerabilities: a national risk assessment

61. Successful implementation of a risk-based approach to combating money-laundering and terrorist financing depends on a sound understanding of the threats and vulnerabilities. Where a country is seeking to introduce a risk-based approach at a national level, this will be greatly aided if there is a national understanding of the risks facing the country. This understanding can flow from a national risk assessment.

62. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of designated competent authorities or SROs and the nature of DNFBPs, including accountants, each country's judgements about the risks will be unique, as will their decisions about how to implement a national assessment in practice. A national assessment need not be a single formal process or document. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and current understanding of the risks. Designated competent authorities, in consultation with the private sector, should consider how best to achieve this while also taking into account any risk associated with providing information on vulnerabilities in their financial systems to money launderers, terrorist financiers, and other criminals.

Principle two: A legal/regulatory framework that supports the application of a risk-based approach

63. Countries should consider whether their legislative and regulatory frameworks are conducive to the application of the risk-based approach. Where appropriate the obligations imposed should be informed by the outcomes of the national risk assessment.

64. The risk-based approach does not mean the absence of a clear statement of what is required from the DNFBPs, including from accountants. However, under a risk-based approach, accountants should have a degree of flexibility to implement policies and procedures which respond appropriately to their own risk assessment. In effect, the standards implemented may be tailored and/or amended by additional measures as appropriate to the risks of an individual firm or business. The fact that policies and procedures, in accordance to the risk levels, may be applied flexibly to different products, services, clients and locations does not mean that policies and procedures need not be clearly defined.

65. Basic minimum AML/CFT requirements can co-exist with a risk-based approach. Indeed, sensible minimum standards, coupled with scope for these to be enhanced when the risk justifies it, should be at the core of risk-based AML/CFT requirements. These standards should, however, be focused on the outcome (combating money laundering and terrorist financing through deterrence, detection, and reporting), rather than applying legal and regulatory requirements in a purely mechanistic manner to every client.

Principle three: Design of a supervisory/monitoring framework to support the application of the risk-based approach

66. Where competent authorities and/or SROs have been assigned responsibility for overseeing AML/CFT controls, countries may wish to consider whether such authorities and SROs are given the necessary authority to implement a risk-based approach to monitoring. Barriers to this may include inappropriate reliance on detailed and prescriptive requirements in the designated competent authorities' or SROs' rules. These requirements may, in turn, stem from the laws under which the designated competent authority or SRO exercises its powers.

67. Where appropriate, designated competent authorities and SROs should seek to adopt a risk-based approach to the monitoring of controls to combat money laundering and terrorist financing. This should be based on a thorough and comprehensive understanding of the types of activity carried out by accountants, and the money laundering and terrorist financing risks to which these are exposed. Designated competent authorities and SROs will probably need to prioritise resources based on their overall assessment of where the risks in accountants' business are.

68. Designated competent authorities and SROs with responsibilities other than those related to AML/CFT will need to consider these risks alongside other risk assessments arising from the competent authority's or SRO's wider duties.

69. Such risk assessments should help a designated competent authority or SRO choose where to apply resources in its supervisory programme, with a view to using limited resources to achieve the greatest effect. Risk assessments may also indicate that a designated competent authority or SRO does not have adequate resources to deal with the risks. In such circumstances, the designated competent authority or SRO may need to obtain additional resources or adopt other strategies to manage or mitigate any unacceptable residual risks.

70. The application of a risk-based approach to monitoring requires that designated competent authorities' and SROs' staff be able to make principles-based decisions in a fashion similar to what would be expected from an accountant or the staff of an accountant's firm. These decisions will cover the adequacy of the arrangements to combat money laundering and terrorist financing. As such, a designated competent authority or SRO may wish to consider how best to train its staff in the practical application of a risk-based approach to monitoring. This staff will need to be well-briefed as to the general principles of a risk-based approach, the possible methods of application, and what a risk-based approach looks like when successfully applied within the context of the national risk assessment.

Principle four: Identifying the main actors and ensuring consistency

71. Countries should consider who the main stakeholders are when adopting a risk-based approach to combating money laundering and terrorist financing. These will differ from country to country. Thought should be given as to the most effective way to share responsibility among these parties, and how information may be shared to best effect. For example, consideration may be given to which body or

bodies are best placed to provide guidance to accountants about how to implement a risk-based approach to anti-money laundering and counter-terrorist financing.

72. A list of potential stakeholders may be considered to include the following:

- Government – This may include legislature, executive, and judiciary.
- Law enforcement agencies – This might include the police, customs and other similar agencies.
- The financial intelligence unit (FIU), security services, and other similar agencies..
- Designated competent authorities/SROs.
- The private sector – This might include accountants and their firms, trade bodies and associations, etc.
- The public – Arrangements designed to counter money laundering and terrorist financing are ultimately designed to protect the law-abiding public. However these arrangements may also act to place burdens on clients of accountants' firms.
- Others – Those who are in a position to contribute to the conceptual basis underpinning the risk-based approach, such stakeholders may include academia and the media.

73. Clearly a government will be able to exert influence more effectively over some of these stakeholders than others. However, regardless of its capacity to influence, a government will be in a position to assess how all stakeholders can be encouraged to support efforts to combat money laundering and terrorist financing.

74. A further element is the role that governments have in seeking to gain recognition of the relevance of a risk-based approach from designated competent authorities and SROs. This may be assisted by relevant authorities making clear and consistent statements on the following issues:

- Accountants can be expected to have flexibility to adjust their internal systems and controls taking into consideration lower and high risks, so long as such systems and controls are reasonable. However, there are also minimum legal and regulatory requirements and elements that apply irrespective of the risk level, for example suspicious transaction reporting and minimum standards of CDD.
- Acknowledging that an accountant's ability to detect and deter money laundering and terrorist financing may sometimes be necessarily limited and that information on risk factors is not always robust or freely available. There can therefore be reasonable policy and monitoring expectations about what an accountant with good controls aimed at preventing money laundering and terrorist financing is able to achieve. An accountant's firm may have acted in good faith to take reasonable and considered steps to prevent money laundering, and documented the rationale for its decisions, and yet still be abused by a criminal.
- Acknowledging that not all high-risk situations are identical and as a result will not always require the application of precisely the same type of enhanced due diligence.

<u>Principle five: Information exchange between the public and private sector</u>

75. Effective information exchange between the public and private sector will form an integral part of a country's strategy for combating money laundering and terrorist financing. In many cases, it will allow

the private sector to provide designated competent authorities and SROs with information they identify as a result of previously provided government intelligence.

76. Public authorities, whether law enforcement agencies, designated competent authorities or other bodies, have privileged access to information that may assist accountants to reach informed judgements when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, accountants are able to understand their clients' businesses reasonably well. It is desirable that public and private bodies work collaboratively to identify what information is valuable to help combat money laundering and terrorist financing, and to develop means by which this information might be shared in a timely and effective manner.

77. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, designated competent authorities and law enforcement agencies should be able to share information and feedback on results and identified vulnerabilities, so that consistent and meaningful inputs can be provided to the private sector. All parties should of course, consider what safeguards are needed to adequately protect sensitive information held by public bodies from being disseminated too widely.

78. Relevant stakeholders should seek to maintain a dialogue so that it is well understood what information has proved useful in combating money laundering and terrorist financing. For example, the types of information that might be usefully shared between the public and private sector would include, if available:

- Assessments of country risk.
- Typologies or assessments of how money launderers and terrorists have abused the DNFBPs, especially accountants.
- Feedback on suspicious transaction reports and other relevant reports.
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards and a country's legal and regulatory framework, it may also be appropriate for authorities to share targeted confidential information with accountants.
- Countries, persons or organisations whose assets or transactions should be frozen.

79. When choosing what information can be properly and profitably shared, public authorities may wish to emphasise to accountants that information from public bodies should inform, but not be a substitute for accountants' own judgements. For example, countries may decide not to create what are perceived to be definitive country-approved lists of low risk client types. Instead, public authorities may prefer to share information on the basis that this will be one input into the accountants' decision making processes, along with any other relevant information that is available.

Chapter Two: Implementation of the Risk-Based Approach

Assessment of risk to inform national priorities

80. A risk-based approach should be built on sound foundations: effort must first be made to ensure that the risks are well understood. As such, a risk-based approach should be based on an assessment of the threats. This is true whenever a risk-based approach is applied, at any level, whether by countries or individual firms. A country's approach should be informed by its efforts to develop an understanding of the risks in that country. This can be considered as a "national risk assessment".

81. A national risk assessment should be regarded as a description of fundamental background information to assist designated competent authorities, law enforcement authorities, the FIU, financial institutions and DNFBPs (including accountants) to ensure that decisions about allocating responsibilities and resources at the national level are based on a practical, comprehensive and up-to-date understanding of the risks.

82. A national risk assessment should be tailored to the circumstances of the individual country, both in how it is executed and in its conclusions. Factors that may influence the risk of money laundering and terrorist financing in a country could include the following:

- Political environment.
- Legal environment.
- A country's economic structure.
- Cultural factors, and the nature of civil society.
- Sources, location and concentration of criminal activity.
- Size and composition of the financial services industry.
- Ownership structure of financial institutions and DNFBPs businesses.
- Size and nature of the activity carried out by DNFBPs, including accountants.
- Corporate governance arrangements in relation to financial institutions, DNFBPs, including accountants, and the wider economy.
- The nature of payment systems and the prevalence of cash-based transactions.
- Geographical spread of the financial industry's and DNFBPs' operations and customers/clients.
- Types of products and services offered by financial institutions and accountants.
- Types of customers/clients serviced by financial institutions and accountants.
- Types of predicate offences.
- Amounts of illicit money generated domestically.
- Amounts of illicit money generated abroad and laundered domestically.
- Main channels or instruments used for laundering or financing terrorism.
- Sectors of the legal economy affected.
- Underground/informal areas in the economy.

83. Countries should also consider how an understanding of the risks of money laundering and terrorist financing can be best achieved at the national level. Relevant questions could include: Which body or bodies will be responsible for contributing to this assessment? How formal should an assessment be? Should a designated competent authority's view, or an SRO's view, be made public? These are all questions for designated competent authority or SRO to consider.

84. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and current understanding of the risks. To achieve the desired outcome, designated competent authorities or SROs should ensure that they identify and provide firms with

the information needed to develop this understanding and to design and implement measures to mitigate the identified risks.

85. Developing and operating a risk-based approach involves forming judgements. It is important that these judgements are well informed. It follows that, to be effective, the risk-based approach should be information-based and include intelligence where appropriate. Effort should be made to ensure that risk assessments are based on fresh and accurate information. Governments, utilising partnerships with law enforcement bodies, FIUs, designated competent authorities/SROs and the accountants themselves, are well placed to bring their knowledge and expertise to bear in developing a risk-based approach that is appropriate for their particular country. Their assessments will not be static and will change over time, depending on how circumstances develop and how the threats evolve. As such, countries should facilitate the sharing of information with different agencies and entities, so that there are no institutional impediments to information dissemination.

86. Whatever form they take, a national assessment of the risks, along with measures to mitigate those risks, can inform how resources are applied to combat money laundering and terrorist financing, taking into account other relevant country policy goals. It can also inform how these resources are most effectively assigned to different public bodies, designated competent authorities and SROs, and how those bodies make use of those resources in an effective manner.

87. As well as assisting designated competent authorities and SROs to decide how to allocate funds to combat money laundering and terrorist financing, a national risk assessment can also inform decision-makers on the best strategies for implementing the regulatory regime to address the risks identified. An over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on industry. Alternatively, less aggressive efforts may not be sufficient to protect societies from the threats posed by criminals and terrorists. A sound understanding of the risks at the national level could help obviate these dangers.

<u>Effective systems for monitoring and ensuring compliance with AML/CFT requirements – General principles</u>

88. FATF Recommendation 24 requires that accountants be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining the design of an effective system, regard may be had to the risk of money laundering or terrorist financing in the sector. There should be a designated competent authority or SRO responsible for monitoring and ensuring its functions, including powers to monitor and sanction. It should be noted that in some countries, accountants are supervised in the same way as financial institutions. Other countries apply a separate monitoring/oversight regime.

Defining the acceptable level of risk

89. The level of AML/CFT risk will generally be affected by both internal and external risk factors. For example, risk levels may be increased by internal risk factors such as weak compliance resources, inadequate risk controls and insufficient senior management involvement. External level risks may rise due to factors such as the action of third parties and/or political and public developments.

90. As described in Section One, all activity involves an element of risk. Designated competent authorities and SROs should not prohibit accountants from conducting business with high risk customers/clients as long as appropriate policies, procedures and processes to manage the attendant risks are in place. Only in specific cases, for example when it is justified by the fight against terrorism, crime or

the implementation of international obligations, are designated individuals, legal entities, organisations or countries categorically denied access to services.

91. However, this does not exclude the need to implement basic minimum requirements. For instance, FATF Recommendation 5 (that applies to accountants through the incorporation of R.5 into R.12) states that "where [the accountant] is unable to comply with (CDD requirements), 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 transaction report in relation to the customer." So the level of risk should strike an appropriate balance between the extremes of not accepting customers/clients, and conducting business with unacceptable or unmitigated risk.

92. Designated competent authorities and SROs expect accountants to put in place effective policies, programmes, procedures and systems to mitigate the risk, and acknowledge that even with effective systems not every suspect transaction will necessarily be detected. They should also ensure that those policies, programmes, procedures and systems are applied effectively to prevent accountants from becoming conduits for illegal proceeds and ensure that they keep records and make reports that are of use to national authorities in combating money laundering and terrorist financing. Efficient policies and procedures will reduce the level of risks, but are unlikely to eliminate them completely. Assessing money laundering and terrorist financing risks requires judgement and is not an exact science. Monitoring aims at detecting unusual or suspicious transactions among an extremely large number of legitimate transactions, furthermore the demarcation of what is unusual may not always be straightforward since what is "customary" may vary depending on the clients' business. This is why developing an accurate client profile is important in managing a risk-based system. Moreover, procedures and controls are frequently based on previous typologies cases, but criminals will adapt their techniques, which may quickly limit the utility of such typologies.

93. Additionally, not all high risk situations are identical, and therefore will not always require precisely the same level of enhanced due diligence. As a result, designated competent authorities/SROs will expect accountants to identify individual high risk categories and apply specific and appropriate mitigation measures. Further information on the identification of specific risk categories is provided in Section Three, "Guidance for Accountants on Implementing the Risk-Based Approach."

Proportionate supervisory/Monitoring actions to support the risk-based approach

94. Designated competent authorities and SROs should seek to identify weaknesses through an effective programme of both on-site and off-site supervision, and through analyses of internal and other available information.

95. In the course of their examinations, designated competent authorities and SROs should review an accountant's AML/CFT risk assessment, as well as its policies, procedures and control systems to arrive at an overall assessment of the risk profile of the accountant's business and the adequacy of its mitigation measures. Where available, assessments carried out by or for accountants may be a useful source of information. The designated competent authority's, or SRO's, assessment of management's ability and willingness to take necessary corrective action is also a critical determining factor. Designated competent authorities and SROs should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe supervisory or monitoring response.

96. Nevertheless, it may happen that the lack of detection of an isolated high risk transaction, or of transactions of an isolated high risk customer/client, will in itself be significant, for instance where the

amounts are significant, or where the money laundering and terrorist financing typology is well known, or where a scheme has remained undetected for a long time. Such a case might indicate an accumulation of weak risk management practices or regulatory breaches regarding the identification of high risks, monitoring, staff training and internal controls, and therefore, might alone justify action to ensure compliance with the AML/CFT requirements.

97. Designated competent authorities and SROs can and should use their knowledge of the risks associated with products, services, clients and geographic locations to help them evaluate the accountants' money laundering and terrorist financing risk assessments, with the understanding, however, that they may possess information that has not been made available to the accountants and, therefore, accountants would not have been able to take such information into account when developing and implementing a risk-based approach. Designated competent authorities and SROs (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist accountants in managing their risks. Where accountants are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by their designated competent authorities and SROs[3]. Guidance designed specifically for accountants is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where accountants use excessively narrow risk categories that do not capture all existing risks, or adopt criteria that lead to the identification of a large number of higher risk relationships, but without providing for adequate additional due diligence measures.

98. In the context of the risk-based approach, the primary focus for designated competent authorities and SROs should be to determine whether or not the accountant's AML/CFT compliance and risk management programme is adequate to: (a) meet the minimum regulatory requirements, and (b) appropriately and effectively mitigate the risks. The monitoring goal is not to prohibit high risk activity, but rather to be confident that firms have adequately and effectively implemented appropriate risk mitigation strategies.

99. Under FATF Recommendation 24, designated competent authorities and SROs should have adequate powers to perform their functions, including the power to impose adequate sanctions for failure to comply with statutory and regulatory requirements to combat money laundering and terrorist financing. Fines and/or penalties are not appropriate in all regulatory actions to correct or remedy AML/CFT deficiencies. However, designated competent authorities and SROs must have the authority and willingness to apply fines and/or penalties in cases where substantial deficiencies exist. Action may also take the form of a remedial program through the normal monitoring processes.

100. In considering the above factors it is clear that proportionate monitoring will be supported by two central features:

a) Regulatory transparency

101. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Designated competent authorities and SROs are aware that accountants, while looking for operational freedom to make their own risk judgements, will also seek guidance on regulatory obligations. As such, the designated competent authority or SRO with AML/CFT supervisory/monitoring responsibilities should seek to be transparent in setting out what it expects, and will need to consider appropriate mechanisms of communicating these messages. For instance, this may be in the form of high-level requirements, based on desired outcomes, rather than detailed processes.

[3] FATF Recommendations 5 and 25, Methodology Essential Criteria 25.1 and 5.12.

102. No matter what individual procedure is adopted, the guiding principle will be that there is an awareness of legal responsibilities and regulatory expectations. In the absence of this transparency there is the danger that monitoring actions may be perceived as either disproportionate or unpredictable which may undermine even the most effective application of the risk-based approach by accountants.

b) Staff Training of designated competent authorities, SROs, and enforcement staff

103. In the context of the risk-based approach, it is not possible to specify precisely what an accountant has to do, in all cases, to meet its regulatory obligations. Thus, a prevailing consideration will be how best to ensure the consistent implementation of predictable and proportionate supervisory/monitoring actions. The effectiveness of supervisory/monitoring training will therefore be important to the successful delivery of proportionate supervisory/monitoring actions.

104. Training should aim to allow designated competent authorities/SRO staff to form sound comparative judgements about AML/CFT systems and controls. It is important in conducting assessments that designated competent authorities and SROs have the ability to make judgements regarding management controls in light of the risks assumed by accountants and their firms and considering available industry practices. Designated competent authorities and SROs might also find it useful to undertake comparative assessments so as to form judgements as to the relative strengths and weaknesses of different accounting firm or business arrangements.

105. The training should include instructing designated competent authorities and SROs about how to evaluate whether senior management has implemented adequate risk management measures, and determine if the necessary procedures and controls are in place. The training should also include reference to specific guidance, where available. Designated competent authorities and SROs also should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

106. To fulfil these responsibilities, training should enable designated competent authorities and SROs monitoring staff to adequately assess:

a. The quality of internal procedures, including ongoing employee training programmes and internal audit, compliance and risk management functions.

b. Whether or not the risk management policies and processes are appropriate in light of the accountants' risk profile, and are periodically adjusted in light of changing risk profiles.

c. The participation of senior management to confirm that they have undertaken adequate risk management, and that the necessary procedures and controls are in place.

SECTION THREE: GUIDANCE FOR ACCOUNTANTS ON IMPLEMENTING A RISK-BASED APPROACH

Chapter One: Risk Categories

107. It is frequently the function of accountants in public practice to assist their clients in managing their affairs in a complex world, providing an individually tailored service. In many circumstances, they will encounter (or recommend) unusual or complex structures as a means of gaining commercial advantage or of dealing in the most appropriate way with complex situations or risks, with no criminal or other ulterior motives. Many factors that to outsiders might be considered indicators of money laundering/terrorist financing (ML/TF) risk, on further examination have an appropriate commercial rationale and the ML/TF risk is in fact normal, rather than high. Nevertheless, accountants will experience higher AML/CFT risk situations, which they need to take into account in their work. In theory, ML/TF risks can be organised into three categories: geographic risk, client risk and service risk. However, in practice these risks may fall into more than one category and should be viewed not as separate and distinct but as inter-related.

108. In the "Client risk" section below, key factors associated with the main client risk category are:

a. Factors indicating that the client is attempting to obscure understanding of its business, ownership or the nature of its transactions.

b. Factors indicating certain transactions, structures, geographical location, international activities or other factors which are not in keeping with the accountant's understanding of the client's business or economic situation. Or

c. Client industries, sectors or categories where opportunities for money laundering or terrorist financing are particularly prevalent.

109. Clients falling within this category may be high risk clients although, after adequate review, the accountant may determine that they are pursuing a legitimate purpose. Provided that the economic rationale for the structure and transactions of a client can be made clear, the accountant may be able to demonstrate that the client is carrying out legitimate operations for which there is a rational and non-criminal purpose.

110. There are also some categories of service provided by practising accountants which may be used by money launderers for their own purposes, and which are therefore subject to a higher degree of risk. These are listed below under "Service Risk".

111. There is no universally accepted set of risk categories, but the examples provided in this Guidance are given for assistance in identifying those that may apply in the circumstances of individual firms or client relationships. There is no one single methodology to apply to these risk categories, and the application of these risk categories is merely intended to provide a suggested framework for approaching the management of potential risks.

Country/Geographic risk

112. There is no universally agreed definition that prescribes whether a particular country or geographic area represents a higher risk. Geographic risk, in conjunction with other risk factors, may provide useful information as to potential money laundering and terrorist financing risks, though it should be borne in mind that lower risk and legitimate commercial enterprises may be located in high risk countries. Nevertheless, clients may be judged to pose a higher than normal risk where they, or their source or destination of funds, are located in a country that is:

- Subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN"). In some circumstances, this would include countries subject to sanctions or measures similar to those issued by bodies such as the UN.
- Identified by credible sources[4] as lacking appropriate AML/CFT laws, regulations and other measures.
- Identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Identified by credible sources as having significant levels of corruption, or other criminal activity.

Client risk

Reduced transparency

113. Factors that may indicate a higher than normal ML/TF risk include:

- Lack of face-to-face introduction of client.
- Subsequent lack of contact, when this would normally be expected.
- Beneficial ownership is unclear.
- Position of intermediaries is unclear.
- Inexplicable changes in ownership.
- Company activities are unclear.
- Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- Management appear to be acting according to instructions of unknown or inappropriate person(s).
- Unnecessarily complex client structure.

[4] "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

- Reason for client choosing the firm is unclear, given the firm's size, location or specialisation.
- Frequent or unexplained change of professional adviser(s) or members of management.
- The client is reluctant to provide all the relevant information or the accountant has reasonable doubt that the provided information is correct or sufficient.

Transactions or Structures out of line with Business Profile

114. Factors that may indicate a higher than normal ML/TF risk include the following:

- Client instructions or funds outside of their personal or business sector profile.
- Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
- Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
- Sudden activity from a previously dormant client.
- Client starts or develops an enterprise with unexpected profile or early results.
- Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
- Clients offer to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

Higher risk sectors and operational structures

115. Some client sectors and operational structures present a higher than normal ML/TF risk. Such risk factors may include:

- Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
- Politically exposed persons.
- Investment in real estate at a higher/lower price than expected.
- Large international payments with no business rationale.
- Unusual financial transactions with unknown source.
- Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.
- Clients incorporated in countries that permit bearer shares.

116. In addition, the existence of fraudulent transactions, or ones which are improperly accounted for, should always be considered high risk. These might include:

- Over and under invoicing of goods/services.

- Multiple invoicing of the same goods/services.
- Falsely described goods/services – Over and under shipments (*e.g.* false entries on bills of lading).
- Multiple trading of goods/services.

Service Risk

117. Services which may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:

- Misuse of pooled client accounts or safe custody of client money or assets.
- Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures).
- Misuse of introductory services, *e.g.* to financial institution.

Variables that May Impact on Risk

118. Some factors that may increase or decrease risk in relation to particular clients, client engagements or practising environments include the following:

- Involvement of financial institutions or other DNFBPs.
- Unexplained urgency of assistance required.
- Sophistication of client, including complexity of control environment.
- Sophistication of transaction/scheme.
- Country location of accountant.
- Working environment/structure of accountant, *e.g.* sole practitioner, large firm.
- Role or oversight of another regulator.
- The regularity or duration of the relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk.
- The purpose of the relationship and the need for the accountant to provide services.
- Clients who have a reputation for probity in the local communities.
- Private companies that are transparent and well know in the public domain.
- The familiarity of the accountant with a country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

Controls for Higher Risk Situations

119. Accountants and accounting firms should implement appropriate measures and controls to mitigate the potential money laundering risks of those clients that are determined to be higher risk as the result of the institution's risk-based approach. These measures and controls may include:

- Increased awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of client teams.
- Increased levels of know your customer (KYC) or enhanced due diligence.
- Escalation for approval of the establishment of a business engagement, or involvement in the client service.

Chapter Two: Application of a Risk-based Approach

Customer due diligence/Know your customer

120. Customer Due Diligence/Know Your Customer is intended to enable an accountant to form a reasonable belief that he knows the true identity of each client and, with an appropriate degree of confidence, knows the types of business and transactions the client is likely to undertake. An accountant's procedures should include procedures to:

(a) Identify and verify the identity of each client on a timely basis.

(b) Identify the beneficial owner, and take reasonable measures to verify the identity of any beneficial owner. The measures which have to be taken to verify the identity of the beneficial owner will vary depending on the risk.

(c) Obtain appropriate additional information to understand the client's circumstances and business, including the expected nature and level of transactions. Relevant customer due diligence information should be periodically updated together with its risk assessment. In the event of any change in beneficial ownership or control of the client, or third parties on whose behalf the client acts, reasonable measures should be taken to verify identity.

121. Practising accountants should thus identify, and verify the identity of their clients, in sufficient detail to provide them with reasonable assurance that the information they have is an appropriate and sufficient indication of the true identity. A standard level of due diligence should be applied to all clients with the possibility to carry out reduced or simplified customer identification in recognised lower risk scenarios. By contrast, an increased level of due diligence will apply in respect to clients that are determined to be of higher risk. These activities may be carried out in conjunction with firms' normal client acceptance procedures, and will take into account any specific jurisdictional requirements for client due diligence. In the normal course of their work, accountants are likely to learn more about some aspects of their client, such as their client's business or occupation and/or their level and source of income, than other advisors. This information is likely to assist in AML/CFT terms.

122. The beneficial owners of the client should be identified, including forming an understanding of the ownership and control structure, and taking reasonable measures to verify the identity of such persons. Public information sources may assist with this requirement. The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominees and complex structures.

123. The types of measures that normally would be needed to satisfactorily perform this function would require identifying:

- The natural persons with a controlling interest.

- The natural persons who comprise the mind and management of the legal person or arrangement.
- Physical location.

124. A risk-based approach varies according to the risk level. For example, where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, and that information is publicly available, fewer checks may be appropriate. In the case of trusts, foundations or similar legal entities where the beneficiaries are distinct from the legal owners of the entity, it will be necessary to form a reasonable level of knowledge and understanding of the classes and nature of the beneficiaries; the identities of the settlor, trustees or managers; and an indication of the purpose of the trust. Assurance will be needed that the declared purpose of the trust is in fact its true purpose.

125. Identification of clients should be reviewed (on an appropriate risk related basis) to ensure that changes in ownership or other factors have not resulted in an effective change in the nature of the client, with a consequent need to review or repeat client identification and verification of identity procedures. This may be carried out in conjunction with any professional requirements for client continuation processes.

Monitoring of client business and transactions for suspicious activity

126. Accountants are not expected to scrutinise every transaction that goes through their clients' books and some accounting services are provided only on a once-off basis, without a continuing relationship with the client. However, many of the professional services provided by accountants put them in a relatively good position to encounter and recognise suspicious activities carried out by their clients or by their clients' business associates, which would not be recognised by other service providers, through their inside knowledge of and access to the client's records and management processes, as well as through close working relationships with senior managers and owners. Practising accountants need to be continually alert for events or situations which are indicative of a reason to be suspicious of money laundering or terrorist financing, employing their professional experience and judgement in the forming of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional accountancy functions and relationships.

127. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that the client retains the same identity and risk profile established initially. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information. As discussed below, ongoing monitoring may also give rise to filing a suspicious transaction report.

128. Investigations into suspected money laundering should not be conducted unless these are within the scope of the engagement, and information is limited to that to which the accountant normally would be entitled in the course of business. Within the scope of engagement, an accountant should be mindful of the proscription on "tipping off" the client where a suspicion has been formulated. Carrying out additional investigations, which are not within the scope of the engagement, is unnecessary and could risk alerting a money launderer.

129. Normal business activities should be maintained and such information or other matters which flow from this will form the proper basis of suspicious transaction reports. To decide whether or not a matter is suspicious, accountants may need to make additional enquiries (within the normal scope of the assignment or business relationship) of the client or their records. Normal commercial enquiries, being made to fulfil duties to clients, may assist in understanding a matter to determine whether or not it is suspicious.

Suspicious activity reporting

130. The requirement to file a suspicious transaction report is not subject to a risk-based approach, but must be made whenever required in the country concerned. This would include both suspicious situations, such as business structures or management profiles which have no legitimate economic rationale and suspicious transactions, such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business.

131. However, it should be noted that a risk-based approach is appropriate for the purpose of identifying a suspicious activity, by directing additional resources at those areas an accountant has identified as higher risk. The designated competent authorities or SROs may provide information to accountants, which will be useful to them to inform their approach for identifying suspicious activity, as part of a risk-based approach. An accountant should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

132. In making a decision on whether to make a report, the following factors will need to be taken into account.

a. Whether or not the activities in question consist of instances of reportable (suspected) money laundering or terrorist financing in the country concerned.

b. Whether the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege (see Recommendation 16). It is for each country to determine the matters that would fall under legal professional privilege or legal professional secrecy.

c. In the absence of a requirement to report a suspicion, in the country concerned, whether it would be permitted to report a suspicion, and whether it would be consistent with the accountants' professional ethical obligations, including the requirement to consider the public interest in carrying out their professional activities.

Accountants should also consider any other specific legal or professional requirements which apply in the country within which the accountant is acting.

133. In many (or most) circumstances, accountants will have no flexibility in judging whether or not a suspicion report should be made, but will find that they are either required to make such a report (by the operation of legal requirements in their country) or forbidden to do so (by the operation of legal or professional requirements). However, where there is any element of flexibility, accountants should take into account the fact that the reporting of suspicious transactions or activities is critical to a country's ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes.

134. The FATF Recommendations require that firms, their partners and employees, should be 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, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Training and awareness

135. Accountants are within the scope of Recommendation 15, which requires firms to provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, accountants

may take account of AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without a professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

Chapter Three: Internal Controls

136. Many DNFBPs differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of DNFBPs have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against ML and FT. For a number of DNFBPs, a single person may be responsible for the functions of front office, back office, money laundering reporting, and senior management. This particularity of DNFBPs, including accountants, should be taken into account in designing a risk-based framework for internal controls systems. The Interpretative Note to Recommendation 15, dealing with internal controls, specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size of the business.

137. In order for accountants to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the firm. The success of internal policies and procedures will be dependent largely on internal control systems. Two key systems that will assist in achieving this objective follow.

Culture of compliance

138. This should encompass:

- Developing, delivering, and maintaining a training program for all accountants.
- Monitoring for any government regulatory changes.
- Undertaking a regularly scheduled review of applicable compliance policies and procedures within accountancy practices, which will help constitute a culture of compliance in the industry.

Senior management ownership and support

139. Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the firm's policies, procedures and processes designed to limit and control risks. Policies and procedures are effective only at the point that firm/company owners and senior management support the policies.

140. Having regard to the size of accounting firm, the framework of internal controls should:

- Provide increased focus on accountants' operations (products, services, clients and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
- Provide for regular review of the risk assessment and management processes, taking into account the environment within which the accountant and the accounting firm operates and the activity in its market place.
- Designate an individual or individuals at management level responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme.

- Ensure that adequate controls are in place before new products are offered.
- Inform senior management of compliance initiatives, and identify compliance deficiencies, corrective action taken, and suspicious activity reports filed.
- Provide for programme continuity despite changes in management or employee composition or structure.
- Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement appropriate risk-based CDD policies, procedures and processes.
- Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enable the timely identification of reportable transactions and ensure accurate filing of required reports.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the firm's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Provide for appropriate training to be given to all relevant staff.
- For groups, to the extent possible, there should be a common control framework.

141. A risk assessment for the firm as a whole, taking into account the size and nature of the practice; the existence of high risk clients (if any); and the provision of high risk services (if any) will be of assistance in setting the required procedures within the firm.

142. Depending on the assessed ML/TF risks, and the size of the firm, it may be possible to simplify both risk assessments and internal procedures. For example, for sole practitioners, client acceptance may be reserved to the sole owner/proprietor taking into account their business and client knowledge and experience (which may be highly specialised). The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, more sophisticated procedures and risk assessments are likely to be necessary.

ANNEXES

ANNEX 1 – SOURCES OF FURTHER INFORMATION

Various sources of information exist that may help governments and accountants in their development of a risk-based approach. Although not an exhaustive list, this section highlights a number of useful web-links that governments and accountants may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such AML/CFT assessments.

A. Financial Action Task Force documents

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. Key resources include the 40 Recommendations on Money Laundering and 9 Special Recommendations on Terrorist Financing, the Methodology for Assessing Compliance with the FATF Recommendations, the Handbook for Countries and Assessors, methods and trends (typologies) reports and mutual evaluation reports.

http://www.fatf-gafi.org

B. Other sources of information to help assist countries' and accountants' risk assessment of countries and cross-border activities

In determining the levels of risks associated with particular country or cross border activity accountants and governments may draw on a range of publicly available information sources, these may include reports that detail observance of international standards and codes, specific risk ratings associated with illicit activity, corruption surveys and levels of international cooperation. Although not an exhaustive list the following are commonly utilised:

- IMF and World Bank Reports on observance of international standards and codes (Financial Sector Assessment Programme)
  - World Bank reports: http://www1.worldbank.org/finance/html/cntrynew2.html
  - International Monetary Fund: http://www.imf.org/external/np/rosc/rosc.asp?sort=topic#RR
  - Offshore Financial Centres (OFCs) IMF staff assessments www.imf.org/external/np/ofca/ofca.asp

- Mutual evaluation reports issued by FATF Style Regional Bodies:

  1. Asia/Pacific Group on Money Laundering (APG)
  http://www.apgml.org/documents/default.aspx?DocumentCategoryID=8

2. Caribbean Financial Action Task Force (CFATF)
http://www.cfatf.org/profiles/profiles.asp

3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
http://www.coe.int/moneyval

4. Eurasian Group (EAG)
http://www.eurasiangroup.org/index-7.htm

5. Financial Action Task Force of South America (GAFISUD)
http://www.gafisud.org/miembros.htm

6. Middle East and North Africa FATF (MENAFATF)
http://www.menafatf.org/TopicList.asp?cType=train

7. The Eastern and South African Anti Money Laundering Group (ESAAMLG)
http://www.esaamlg.org/

8. *Groupe Inter-gouvernemental d'Action contre le Blanchiment d'Argent* (GIABA)
http://www.giabasn.org

- OECD Sub Group of Country Risk Classification (a list of country risk classifications published after each meeting)
http://www.oecd.org/document/49/0,2340,en_2649_34171_1901105_1_1_1_1,00.html
- International Narcotics Control Strategy Report (published annually by the US State Department)
http://www.state.gov/p/inl/rls/nrcrpt/
- Egmont Group membership – Coalition of FIU's that participate in regular information exchange and the sharing of good practice, acceptance as a member of the Egmont Group is based a formal procedure that countries must go through in order to be acknowledged as meeting the Egmont definition of an FIU.
http://www.egmontgroup.org/
- Signatory to the United Nations Convention against Transnational Organized Crime
http://www.unodc.org/unodc/crime_cicp_signatures_convention.html
- The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury, Economic and Trade Sanctions Programmes
http://www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml
- Consolidated list of persons, groups and entities subject to EU Financial Sanctions
http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm
- UN Security Council Sanctions Committee - Country Status:
http://www.un.org/sc/committees/

ANNEX 2 – GLOSSARY OF TERMINOLOGY

Beneficial Owner

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.

Competent authorities

Competent authorities refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

Country

All references in the FATF Recommendations and in this Guidance to *country* or *countries* apply equally to territories or jurisdictions.

Designated Non-Financial Businesses and Professions

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.

FATF Recommendations

Refers to the FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing.

Identification data

Reliable, independent source documents, data or information will be referred to as "identification data".

Politically Exposed Persons (PEPs)

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.

Self-regulatory organisation (SRO)

A *SRO* is a body that represents a profession (*e.g.* lawyers, notaries, other independent legal professionals or accountants), and which is made up of member professionals, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

ANNEX 3 – MEMBERS OF THE ELECTRONIC ADVISORY GROUP

FATF and FSRB members and observers

Argentina; Asia Pacific Group (APG); Australia; Belgium; Azerbaijan; Canada; Chinese Taipei, China; European Commission (EC); Nigeria; France; Hong Kong, China; Italy; Japan; Luxembourg; MONEYVAL; Netherlands; New Zealand; Offshore Group of Banking Supervisors (OGBS); Portugal; Romania; Spain; South Africa; Switzerland; United Kingdom; United States.

Dealers in precious metals and dealers in precious stones industries

Antwerp World Diamond Centre, International Precious Metals Institute, World Jewellery Confederation, Royal Canadian Mint, Jewellers Vigilance Committee, World Federation of Diamond Bourses, Canadian Jewellers Association.

Real estate industry

International Consortium of Real Estate Agents, National Association of Estate Agents (UK), the Association of Swedish Real Estate Agents.

Trust and company service providers industry

The Society of Trust and Estate Practitioners (STEP), the Law Debenture Trust Corporation.

Accountants industry

American Institute of Certified Public Accountants, Canadian Institute of Chartered Accountants, European Federation of Accountants, German Institute of Auditors, Hong Kong Institute of Public Accountants, Institute of Chartered Accountants of England & Wales.

Casinos industry

European Casino Association (ECA), Gibraltar Regulatory Authority, Kyte Consultants (Malta), MGM Grand Hotel & Casino, Unibet, William Hill plc.

Lawyers and notaries

Allens Arther Robinson, American Bar Association, American College of Trust and Estate Council, Consejo General del Notariado (Spain), Council of Bars and Law Societies of Europe (CCBE), International Bar Association (IBA), Law Society of England & Wales, Law Society of Upper Canada.