Financial Action Task Force

Groupe d'action financière

RBA GUIDANCE FOR TRUST AND COMPANIES SERVICE PROVIDERS (TCSPs)

17 June 2008

TABLE OF CONTENTS

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

HIGH LEVEL PRINCIPLES AND PROCEDURES FOR TRUST AND COMPANY SERVICE PROVIDERS (TCSPS)

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 organisations which represent lawyers, notaries, accountants, trust and company service providers, 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 trust and company service providers (TCSPs) 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 is presented in a way that is focused and relevant for TCSPs. 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, in addition to specialised trust and company service providers, financial institutions, lawyers, and accountants may also undertake the trust and company services covered by the Recommendations.

9. DNFBPs provide a range of services and activities that differ vastly, *e.g.* in their methods of delivery, in the depth and duration of the relationships formed with customers, and the size of the operation. For example, some of these entities are single person operations. This Guidance is written at a high level to cater for the differing practices of TCSPs 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 TCSPs and other DNFBP sectors that will be mutually beneficial to combating money laundering and terrorist financing.

10. The FATF definition of TCSP relates to providers of trust and company services that are not covered elsewhere by the FATF Recommendations, and therefore excludes financial institutions, lawyers, notaries, other independent legal professionals and accountants. Separate guidance is being issued for those sectors, and they should therefore apply that guidance. However, all those engaged in TCSP activities may also wish to refer to the TCSPs guidance, as it is more specifically tailored to TCSP services.

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

12. FATF 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 TCSPs when they prepare for and carry out transactions for a client in relation to the following activities:

- Acting as a formation agent of legal persons.

- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
- Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement.
- Acting as (or arranging for another person to act as) a trustee of an express trust.
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

13. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions (see paragraphs 116-118) 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 DNFBPs subject to the certain qualifications. Specifically, Recommendation 16 applies to trust and company service providers when they prepare for or carry out a transaction on behalf of a client, in relation to the activities referred to at R.12 above.

14. The wider audience for this guidance includes countries, regulators, and self regulatory organisations (SROs), which are considering how to apply AML/CFT measures to TCSPs. Countries need to identify the most appropriate regime, tailored to address individual country risks, which takes into consideration the idiosyncrasies and activities of TCSPs and the 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.

Observation on the particular activities carried out by TCSPs

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

16. TCSPs can take different forms. In some countries they may be predominantly lawyers. In other countries–particularly in countries with a high concentration of non-resident business–TCSPs are independent trust companies or are trust companies that are subsidiaries of banks, and may be other professionals such as accountants. In other countries, trust service providers (*e.g.* trust companies) and company service providers are separate and distinct categories of entities subject to separate regulatory requirements. As a result, not all persons and businesses active in the TCSP industries provide all of the services listed in the definition of a TCSP. Accordingly, risk should be identified and managed on a service-by-service basis.

Chapter Two: The Risk-Based Approach – Purpose, benefits and challenges

The purpose of the risk-based approach

17. The FATF Recommendations contain language that permits countries to some degree 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.

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

19. A number of the DNFBP sectors, including TCSPs, are already subject to regulatory or professional requirements which complement AML/CFT measures. Where possible, it will be beneficial for TCSPs 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 the honest customers can access the services provided by TCSPs, but creates barriers to those who seek to misuse these services.

20. 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. TCSPs will need this assistance to help them to identify higher risk customers, products and services, including delivery channels, and geographical locations. These are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve.

21. 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 so as to facilitate investigations.

22. 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.

23. 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.

24. An effective risk-based approach will allow TCSPs to exercise reasonable business and professional judgement with respect to customers. 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 TCSPs from continuing with legitimate business or from finding innovative ways to diversify their business.

25. 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 are more likely to target the DNFBP sectors, including TCSPs, if other routes become more difficult. For this reason, DNFBPs 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 TCSPs, to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

26. 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

27. 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 customers. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively.

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

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

Challenges

30. A risk-based approach is not necessarily an easy option, and there may be challenges to overcome 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 42-46 below.

31. 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 lack of understanding by customers regarding information required.

32. Implementing a risk-based approach requires that TCSPs 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. TCSPs may overestimate risk, which could lead to wasteful use of resources, or they may underestimate risk, thereby creating vulnerabilities.

33. TCSPs 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. 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.

34. Designated competent authorities and SROs should place greater emphasis on whether a TCSP has 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 a TCSP'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 that was not reasonably available at the time.

35. In implementing the risk-based approach, TCSPs should be given the opportunity to make reasonable judgements with respect to their particular situations. This may mean that no two TCSPs or no two businesses are likely to adopt the same detailed practices. Such potential diversity of practice will require that designated competent authorities and SROs make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges for 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 authority or an SRO in determining whether a TCSP has made sound risk-based judgements.

36. 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

37. The varying degrees of risk of money laundering or terrorist financing for particular types of DNFBPs, including TCSPs, or for particular types of customers 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)**.**

38. 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 TCSPs, 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 TCSPs (*R.24*).

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

39. Risk is referred to in several forms:

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

b) Lower risk – A country may also permit its DNFBPs, including TCSPs, to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). TCSPs 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 TCSPs, 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 or SROs assess or review the procedures adopted by TCSPs 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 applies. In addition, where the designated competent authorities or 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)

40. 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 customers, 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 TCSPs, to have regard to the 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)

41. Countries should ensure that TCSPs 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.

Applicability of the risk-based approach to terrorist financing

42. 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 make its detection difficult and the implementation of mitigation strategies may be 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.

43. 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 TCSPs to determine the type of underlying criminal activity, or intended terrorist purpose; rather, the TCSP'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.

44. The ability of TCSPs 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).

45. 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 TCSPs to comply with those sanctions are decided by individual countries and are not a function of risk. TCSPs may commit a criminal offence if they undertake a business with a listed individual, organisation or country, or its agent, in contravention of applicable sanctions.

46. For these reasons, this Guidance has not comprehensively addressed the application of a risk-based process 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 TCSPs, 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

47. 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.

48. 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 116-118.

49. There are several components of customer due diligence – identification and verification of the 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 the 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.

50. Countries may allow TCSPs 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 customer due diligence. 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 customer identity, such as customer location, may be needed to adequately assess risk. This will be an iterative process: the preliminary information obtained about a customer should be sufficient to determine whether to go further, and in many cases customer monitoring will provide additional information.

51. Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk customers, monitoring is needed to verify that transactions match the initial low risk profile and if not, trigger a process for appropriately revising the customer's risk rating. Equally, risks for some customers may only become evident once a relationship with a customer has begun. This makes appropriate and reasonable monitoring of customer 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 customers 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

52. Risk-based policies and processes should be distinguished from risk-based monitoring by designated competent authorities or SROs. There is a general recognition within supervisory/monitoring practice that resources should be allocated taking into account the risks posed by individual 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 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 businesses are exposed. Consequently, this prioritisation should lead designated competent authorities or SROs to focus increased regulatory attention on businesses that engage in activities assessed to present a higher risk of money laundering or terrorist financing.

53. 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.

54. Since designated competent authorities or SROs should have already assessed the quality of risk management controls applied throughout TCSPs, 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

- TCSPs, designated competent authorities or SROs should have access to reliable and actionable information about the threats.
- 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 TCSPs need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Designated competent authorities' or SROs' supervisory staff must be well-trained in the risk-based approach, both as applied by designated competent authorities/SRO and by TCSPs.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

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

55. The application of a risk-based approach to countering money laundering and the financing of terrorism will allow designated competent authorities or SROs and TCSPs 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.

56. 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 is appropriate to the particular circumstances of the country in question.

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

57. 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.

58. 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 TCSPs, 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 and SROs, 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 and non-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

59. 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.

60. The risk-based approach does not mean the absence of a clear statement of what is required from the DNFBPs, including from TCSPs. However, under a risk-based approach, TCSPs 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 business. The fact that policies and procedures, in

accordance to the risk levels, may be applied to different products, services, customers[1] and locations does not mean that policies and procedures need not be clearly defined.

61. Basic minimum AML 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 through deterrence, detection, and reporting of money laundering and terrorist financing), rather than applying legal and regulatory requirements in a purely mechanistic manner to every customer.

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

62. Where designated competent authorities 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.

63. 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 TCSPs, 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 the TCSP's business are.

64. 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 designated competent authority's or SRO's wider duties.

65. Such risk assessments should help the designated competent authority or SRO choose where to apply resources in its monitoring programme, with a view to using limited resources to achieve the greatest effect. A risk assessment may also indicate that the 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.

66. The application of a risk-based approach to monitoring requires that designated competent authorities' and SROs' staff be able to make principle-based decisions in a fashion similar to what would be expected from a TCSP or the staff of a TCSP's business. 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

67. 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

[1] For TCSPs, the term "client" is often considered more appropriate; references to "customer" include the concept of client.

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 TCSPs about how to implement a risk-based approach to AML/CFT.

68. A list of potential stakeholders may include the following:

- Government – This may include legislature, executive, and judiciary.
- Law enforcement agencies – This might include the police, custom and similar agencies.
- The financial intelligence unit (FIU), security services, and other similar agencies.
- Designated competent authorities/SROs.
- The private sector – This might include TCSPs and their firms, national and international 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 customers of TCSPs' businesses.
- 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.

69. 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.

70. 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:

- TCSPs 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 customer due diligence.
- Acknowledging that a TCSP'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 a TCSP with good controls aimed at preventing money laundering and the financing of terrorism is able to achieve. A TCSP 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.

Principle five: Information exchange between the public and private sector

71. 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.

72. Public authorities, whether law enforcement agencies, designated competent authorities or other bodies, have privileged access to information that may assist TCSPs to reach informed judgements when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, TCSPs 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.

73. 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.

74. 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 TCSPs.
- 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 TCSPs.
- Countries, persons or organisations whose assets or transactions should be frozen.

75. When choosing what information can be properly and profitably shared, public authorities may wish to emphasize to TCSPs that information from public bodies should inform, but not be a substitute for, TCSPs' own judgements. For example, countries may decide not to create what are perceived to be definitive country-approved lists of low risk customer types. Instead, public authorities may prefer to share information on the basis that this will be one input into TCSPs' 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

76. 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".

77. 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 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.

78. A national risk assessment should be tailored to the circumstances of the individual country, both in how it is executed and 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 TCSPs (this applies particularly to company incorporation for non-residents).
- Corporate governance arrangements in relation to financial institutions and DNFBPs 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
- Types of products and services offered by the financial services industry and DNFBPs
- Types of customers serviced by financial institutions and DNFBPs.
- 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.

79. 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 the designated competent authority's or SRO's view be made public? These are all questions for the designated competent authority or SRO to consider.

80. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and up-to-date 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.

81. 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 TCSPs 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 flow of information between different bodies, so that there are no institutional impediments to information dissemination.

82. 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 and SROs, and how those bodies make use of those resources in an effective manner.

83. 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.

Effective systems for monitoring and ensuring compliance with AML/CFT requirements – General Principles

84. FATF Recommendation 24 requires that TCSPs be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. In determining the 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 compliance of TCSPs; the authority or SRO should have adequate powers to perform its functions, including powers to monitor and sanction. It should be noted that in some countries, TCSPs are supervised in the same way as banks and other financial institutions. Other countries apply a separate monitoring/oversight regime.

Defining the acceptable level of risk

85. 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.

86. As described in Section One, all activity involves an element of risk. Designated competent authorities and SROs should not prohibit TCSPs from conducting business with high risk customers 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 denied categorically access to services.

87. However, this does not exclude the need to implement basic minimum requirements. For instance, FATF Recommendation 5 (that applies to TCSPs through the incorporation of R.5 into R.12) states that "where [the TCSP] 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, and conducting business with unacceptable or unmitigated risk.

88. Where TCSPs are allowed to implement a risk-based approach, designated competent authorities and SROs expect TCSPs 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 TCSPs 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 customers' business. This is why developing an accurate customer 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.

89. 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 TCSPs 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 Trust and Company Service Providers on Implementing a Risk-Based Approach."

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

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

91. In the course of their examinations, designated competent authorities and SROs should review a TCSP's AML/CFT risk assessments as well as its policies, procedures and control systems to arrive at an overall assessment of the risk profile of TCSPs' business and the adequacy of its mitigation measures. Where available, assessments carried out by or for TCSPs may be a useful source of information. The designated competent authority/SRO 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 monitoring response.

92. Nevertheless, it may happen that the lack of detection of an isolated high risk transaction, or of transactions of an isolated high risk customer, 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.

93. Designated competent authorities and SROs can and should use their knowledge of the risks associated with products, services, customers and geographic locations to help them evaluate TCSPs' money laundering and terrorist financing risk assessments, with the understanding, however, that they may possess information that has not been made available to TCSPs and, therefore, TCSPs 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 TCSPs in managing their risks. Where

TCSPs 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[2]. Guidance designed specifically for TCSPs is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where TCSPs 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.

94. 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 TCSP'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.

95. 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. Often, action will take the form of a remedial program through the normal monitoring processes.

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

a) Regulatory Transparency

97. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Designated competent authorities and SROs are aware that TCSPs, while looking for operational freedom to make their own risk judgements, will also seek guidance on regulatory obligations. As such, the designated competent authority/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.

98. 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 TCSPs.

b) Staff Training of Designated Competent Authorities, SROs, and Enforcement Staff

99. In the context of the risk-based approach, it is not possible to specify precisely what a TCSP 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 monitoring actions. The effectiveness of monitoring training will therefore be important to the successful delivery of proportionate supervisory/monitoring actions.

100. 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 TCSPs and their firms and considering

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

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 firms or business arrangements.

101. 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.

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

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

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

iii. 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 TRUST AND COMPANY SERVICE PROVIDERS (TCSPS) ON IMPLEMENTING A RISK-BASED APPROACH

Chapter One: Risk Categories

103. In order to implement a reasonable risk-based approach, TCSPs should identify the criteria to assess potential money laundering and terrorist financing risks on a service-by-service basis. These risks will vary according to the activities undertaken by the TCSP.

104. Identification of the money laundering and terrorist financing risks, to the extent that such terrorist financing risk can be identified, of customers or categories of customers, and transactions will allow TCSPs to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident through time, making monitoring of customer transactions and ongoing reviews a fundamental component of a reasonably designed risk-based approach. A TCSP may also have to adjust its risk assessment of a particular customer based upon information received from a designated competent authority or SRO.

105. Money laundering and terrorist financing risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling TCSPs to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer risk; and product/services risk. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one TCSP to another, depending upon their respective circumstances. Consequently, TCSPs will have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a TCSP's discretion.

106. While there is no agreed upon set of risk categories for TCSPs, the examples provided herein are the most commonly identified risk categories. There is no one single methodology for applying these risk categories; however, the application of these risk categories is intended to assist in designing an effective strategy for managing the potential risks.

Countries/Geographic risk

107. There is no universally agreed definition by either competent authorities or TCSPs that prescribes whether a particular country or geographic area (including the country within which the TCSP operates) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing vulnerabilities. Factors that may result in the determination that a country poses a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognised, may be given credence by a TCSP because of the standing of the issuer and the nature of the measures.

- Countries identified by credible sources[3] as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

Customer risk

108. Determining the potential money laundering or terrorist financing risks, to the extent that such terrorist financing risks can be identified, posed by a customer, or category of customers, is critical to the development of an overall risk framework. Based on its own criteria, a TCSP will determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include:

- Customers[4] conducting their business relationship or transactions in unusual circumstances, such as:
  - Significant and unexplained geographic distance between the TCSP and the location of the customer.
- Customers where the structure or nature of the entity or relationship makes it difficult to identify and verify the true owner or controlling interests, such as:
  - Unexplained use of corporate structures, express trusts and nominee shares, and use of bearer shares.
  - Unexplained delegation of authority by the applicant or customer through the use of powers of attorney, mixed boards and representative offices.
  - Unexplained relationship between an applicant's beneficial owners and controllers and account signatories.
  - In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
  - In the case of an express trust, an unexplained nature of classes of beneficiaries and classes within an expression of wishes.
- Cash (and cash equivalent) intensive businesses including:

---

3 "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.

4 TCSPs generally use the term "client" instead of "customer." The definition of "client" of the TCSP, may extend (for identification and verification purposes) to other relevant parties who might have some degree of control over the trust/company structure. This should include the settlor, the trustee or person exercising effective control over the trust and the beneficiaries. This may include protectors if they have any positive powers. Nevertheless it is generally accepted that not all beneficiaries are always beneficial owners. Different countries have adopted different approaches to deal with this issue.

- Money services businesses (*e.g.* remittance houses, currency exchange houses, casas de cambio, bureau de change, money transfer agents and bank note traders or other businesses offering money transfer facilities
- Casinos, betting and other gambling related activities.
- Businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions.

- Charities and other "not for profit" organisations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis).
- Other TCSPs, financial institutions, and other designated non-professional businesses and professions who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised.
- Customers that are politically exposed persons (PEPs).
- Customers where there is no commercial rationale for a customer buying the products or services that he seeks, who request undue levels of secrecy, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered.

Product/Service risk

109. An overall risk assessment should also include determining the potential risk presented by products and services offered by a TCSP. TCSPs should be mindful of the risks associated with new or innovative products or services. A key element for TCSPs is establishing the existence of an apparent legitimate business, economic, tax or legal reasons for the structures the TCSP is asked to set up and manage. Determining the risks of products and services should include the consideration of such factors as:

- Shell companies, companies with ownership through nominee shareholding and control through nominee and corporate directors[5].
- Services where TCSPs, acting as financial intermediaries, actually handle the receipt and transmission of cash proceeds through accounts they actually control in the act of closing a business transaction.
- Other services to conceal improperly beneficial ownership from competent authorities.
- Situations where it is difficult to identify the beneficiaries of trusts. This might include situations where identification is hindered because the beneficiary of a trust is another trust or corporate vehicle, or where the trust deed does not include the names of the settlor, the beneficiaries or the class of beneficiaries.[6]
- Commercial, private, or real property transactions or services with no apparent legitimate business, economic, tax, family governance, or legal reasons.
- Payments received from unassociated or unknown third parties where this would not be a typical method of payment.
- The offer by customers to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Services that inherently have provided more anonymity.

---

[5] See detailed examples of the use of these types of products in the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers" published 13 October 2006.

[6] See the FATF typologies report "The Misuse of Corporate Vehicles, including Trust and Company Service Providers," Annex 2 on trusts, for a more detailed description of "potential for misuse" of trusts.

- Trusts which are pensions that may be considered lower risk.

Variables that may impact risk

110. A TCSP's risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease perceived risks posed by a particular customer or transaction and may include:

- The purpose and intended nature of a relationship.
- The type, volume and value of activity expected.
- The source of funds and the source of wealth – the source of funds is the activity that generates the funds for a customer, while the source of wealth describes the activities which have generated the total net worth of a customer.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow for a TCSP to treat the customer as lower risk.
- The level of regulation or other oversight of a government's regime to which a customer is subject. A customer that is a financial institution regulated in a country with a satisfactory AML regime poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation. Additionally, companies and their wholly owned subsidiaries that are publically owned and traded on a recognised exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate, recognised regulatory scheme, and, therefore, generally pose less risk due to the type of business that they conduct and the wider government's regime to which they are subject.
- The regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from the money laundering perspective.
- The familiarity with the country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as a result of a TCSPs own operations within the country.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that will increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

Controls for higher risk situations

111. TCSPs should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as a result of the TCSP's risk assessment. The same measures and controls may often address more than one of the risk criteria identified and it is not necessarily expected that a TCSP establish specific controls targeting each and every criteria. Appropriate measures and controls may include:

- General training on money laundering and terrorist financing methods and risks relevant to TCSPs.
- Targeted training for increased awareness of higher risk customers and transactions.

- Increased levels of customer due diligence or enhanced due diligence.
- Escalation of the approval of the establishment of a relationship.
- Increased monitoring of the services offered to determine whether the risk of money laundering occurring has increased.
- Increased levels of ongoing controls and frequency of reviews of relationships.

Chapter Two: Application of a Risk-based Approach

Customer due diligence/know your customer

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

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

(b) Identify the beneficial owner, and take reasonable measures to verify the identity of any beneficial owner. The measures that 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 customer'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 applicant, or third parties on whose behalf the applicant acts, reasonable measures should be taken to verify identity.

113. The starting point is for a TCSP to assess the risks that a customer may pose taking into consideration any appropriate risk variables before making a final determination. TCSPs will determine the due diligence requirements appropriate to each customer. This may include:

- A standard level of due diligence, to be applied to all customers.
- The standard level being reduced in recognised lower risk scenarios, such as:
  - Publicly listed companies subject to regulatory disclosure requirements.
  - Financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.
- An increased level of due diligence in respect of those customers that are determined to be of higher risk. This may be the result of a customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing a higher risk, such as:
  - PEPs.
  - Sanctioned countries.

Monitoring of customers and transactions

114. The degree and nature of monitoring by a TCSP will depend on the size of the TCSP, the AML/CFT risks that the institution has identified, the monitoring method being used (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, TCSPs and where appropriate their regulatory supervisors must recognise that

not all transactions or customers will be monitored in the same way. The degree of monitoring will be based on the perceived risks associated with the customer, the products or services being used by the customer, the location of the customer, and the particular transaction. Monitoring methodologies and processes also need to take into account the resources of the TCSP.

115. Monitoring under a risk-based approach allows a TCSP to determine which activity need not be reviewed or reviewed less frequently. Defined situations used for this purpose should be reviewed on a regular basis to determine the adequacy for the risk levels established. TCSPs should also assess the adequacy of any systems and processes on a periodic basis. The results of such monitoring should always be documented.

Suspicious transaction reporting

116. The reporting of suspicious transactions or activities is critical to a country's ability to utilise financial information to combat money laundering, terrorist financing, and other financial crimes. Countries' reporting regimes are laid down in national law, requiring institutions to file reports when the threshold of suspicion is reached. A TCSP's requirement to report a suspicious transaction will arise when the TCSP engages in a transaction for a client, or on behalf of a client, in relation to the activities referred to in the Glossary to the FATF Recommendations. (See paragraphs 12-13.)

117. Where a legal or regulatory requirement mandates the reporting of a suspicious activity once the suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of a suspicious activity under these circumstances is not applicable.

118. A risk-based approach is, however, appropriate for the purpose of identifying a suspicious activity, for example, by directing additional resources at those areas a TCSP has identified as higher risk. As part of a risk-based approach, it is also likely that a TCSP will utilise information provided by designated competent authorities or SROs to inform its approach to identifying suspicious activity. A TCSP should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

Training and awareness

119. FATF Recommendations 15 and 16 together require that TCSPs provide their employees with AML/CFT training, and it is important that TCSP employees receive appropriate and proportionate training with regard to money laundering and terrorist financing. A TCSP's commitment to having successful controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees with at least general information on AML/CFT laws, regulations and internal policies.

120. Applying a risk-based approach to the various methods available for training, however, gives each TCSP additional flexibility regarding the frequency, delivery and focus of such training. A TCSP should review its own workforce and available resources and implement training programmes that provide appropriate AML/CFT information that is:

- Tailored to the appropriate staff responsibility (*e.g.* customer contact or operations).
- At the appropriate level of detail (*e.g.* frontline personnel, complicated products or customer managed products).
- At a frequency related to the risk level of the business involved.
- Tested to assess staff knowledge commensurate with the detail of information provided.

Chapter Three: Internal Controls

121. 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 money laundering and terrorist financing. 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 TCSPs, 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.

122. In order for TCSPs to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the institutions. Senior management is ultimately responsible for ensuring that a TCSP maintains an effective internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and engagement in AML 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 TSCPs policies, procedures and processes designed to limit and control risks.

123. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will depend upon a number of factors including:

- The nature, scale and complexity of a TSCP's business.
- The diversity of a TCSP's operations, including geographical diversity.
- The TCSP's customer, product and activity profile.
- The volume and size of the transactions.
- The degree of risk associated with each area of the TCSP's operation.
- The extent to which the TCSP is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non face-to-face access.
- The frequency of customer contact (either in person or by other means of communication).

124. Having regard to the size of the TCSP, the framework of internal controls should generally:

- Provide increased focus on a TCSP's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
- Provide for a regular review of the risk assessment and management processes, taking into account the environment within which the TSCP 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 or services are offered.
- Inform senior management of compliance initiatives, identified 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 where appropriate, all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence policies, procedures and processes.
- Provide for adequate controls for higher risk customers, transactions and products/services, 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 transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the institution'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.

125. Senior management will need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of the TCSP. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the TCSP's AML/CFT compliance programme. The testing should be risk-based (focussing attention on higher risk customers, products and services) and include comprehensive procedures and testing that cover all activities. It should also evaluate the adequacy of the TCSP's overall AML/CFT programme and the quality of its operational risk management programme.

ANNEXES

ANNEX 1 – SOURCES OF FURTHER INFORMATION

Various sources of information exist that may help governments and TCSPs 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 TCSPs 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 TCSPs' risk assessment of countries and cross-border activities

In determining the levels of risks associated with particular country or cross border activity, TCSPs 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. 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 of 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 (DNFBPs)

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.

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document *e.g.* a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (*e.g.* constructive trust).

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".

Legal Persons

Legal persons refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

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.