FATF • GAFI

Financial Action Task Force Groupe d'action financière

FATF Report

Risk-Based Approach

Guidance for Money Service Businesses

July 2009

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

SECTION ONE: USING THE GUIDANCE & PURPOSE OF THE RISK-BASED APPROACH ...5

Chapter One: Background and Context 5
Purpose of the Guidance: 5
Target Audience, Status and Content of the Guidance: 6
Chapter Two: The Risk-Based Approach – *purpose, benefits and challenges* 7
The purpose of the Risk-Based Approach....7
Potential Benefits and Challenges of the Risk-Based Approach....8
Chapter Three: FATF and the Risk-Based Approach....10
General Risk Principle 10
Specific Risk References....10
Applicability of the risk-based approach to terrorist financing....13
Limitations to the risk-based approach 14
Distinguishing Risk-Based Supervision and Risk-Based Policies and Processes....15

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES 16

Chapter One: High-level principles for creating a risk-based approach 16
Principle One: Understanding and responding to the threats and vulnerabilities: a national risk assessment....16
Principle Two: A legal/regulatory framework that supports the application of a risk-based approach 16
Principle Three: Design of a supervisory framework to support the application of the risk-based approach 17
Principle Four: Identifying the main actors and ensuring consistency....17
Principle Five: Information exchange between the public and private sector 19
Chapter Two: Implementation of the Risk-Based Approach 20
Assessment of Risk to Inform National Priorities....20
Regulatory Supervision – General Principles 21

SECTION THREE: GUIDANCE FOR MONEY SERVICES BUSINESSES ON IMPLEMENTING A RISK-BASED APPROACH 26

Preamble 26
Chapter One: Risk Categories....28
Country/Geographic Risk....28
Customer Risk 29
Product / Transaction / Service Risk 30
Agents Risk 32
Variables That May Impact Risk....33
Controls for Higher Risk Situations 34
Chapter Two: Application of a Risk-Based Approach 35
Customer Due Diligence/Know Your Customer....35
Monitoring of Customers and Transactions 37
Suspicious Transaction Reporting....37

Training and Awareness 38
Agent Due Diligence / Know Your Agent 38
Agent Monitoring 40
Training and Awareness 41
Chapter Three: Internal Controls 42
REFERENCES 44
ANNEX 1 SOURCES OF FURTHER INFORMATION 45
A. Financial Action Task Force Documents 45
B. Legislation/Guidance on the Risk-Based Approach 45
C. Other Sources of Information to help assist national and financial institution risk assessment of countries and cross border activities 46
ANNEX 2 GLOSSARY OF TERMINOLOGY 49
ANNEX 3 MEMBERSHIP OF THE ELECTRONIC ADVISORY GROUP 53

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 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 2008, the FATF adopted Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures for the Accountants, Casinos, Dealers in Precious Metals and Dealers in Precious Stones, Legal Professionals, Real Estate Agents, and Trust and Company Service Providers.

3. A meeting was held in September 2008 and was attended by organisations representing money services businesses (MSB). An Electronic Advisory Group (EAG) was established for this process and was chaired by Mr. Ezra Levine (The Money Services Round Table, United States). Membership of the Group has consisted of FATF members and observers, as well as representatives from the MSB sectors that volunteered to work on the issue of the risk-based approach to combating money laundering and terrorist financing. A list of members is attached at Annex 3.

4. After further international consultation with both public and private sectors, the FATF adopted RBA Guidance for the money services businesses at its June 2009 Plenary.

Purpose of the Guidance:

5. 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 public and private sector practice in the design and implementation of an effective risk-based approach.

6. 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.

Target Audience, Status and Content of the Guidance:

7. The Guidance is primarily addressed to public authorities and MSBs. MSBs generally provide a subset of the financial services provided by financial institutions. This Guidance focuses on the transfer of money or value and money and currency changing operated by MSBs.

8. Money/value transfer companies provide an essential financial service, often in underdeveloped regions with limited or no banking services. Money/value transfer companies operate in a variety of ways, but typically a sending agent accepts payment of the money transfer (including a fee), collects the required identification information, and enters the transaction and sender's applicable identification information and the destined receiver systematically at the point of origination. In the case of international locations and multiple currencies, foreign exchange rates are applied and converted systematically. The money transfer is made available to the ultimate recipient, in the appropriate currency, at a receiving agent location in the paying jurisdiction. Payout methods vary by jurisdiction, but may include cash, cheque, money order, payout cards, bank deposit or a combination.

9. Money/currency exchange dealers engage in the business of accepting the currency or other monetary instruments denominated in the currency of one country, in exchange for the currency or other monetary instruments denominated in the currency of one or more other countries.

10. The MSB sector is made up of a very diverse group of organisations. A MSB may be a small organisation with outlet locations such as grocery stores, drugstores, pharmacies or convenience stores. It may also include a regional network of post offices or banks or other MSBs, which can be branches or agents. In considering how to implement a risk-based approach in the MSB sector, public authorities may wish to consider providing a simplified version of this guidance for small and less-complex MSBs.

11. The overall document is structured into three interdependent sections. Section one sets out the key elements of the risk-based approach and provides the basis for interpreting section two (Guidance for Public Authorities) and section three (Guidance for Money Services Businesses). There is also Annex 1, which contains descriptions of additional sources of information.

12. The Guidance aims to set out the key elements of an effective risk-based approach and identifies the types of issues that both public authorities and MSBs may wish to consider when applying a risk-based approach.

13. The Guidance recognises that each country and its national authorities, in partnership with its MSBs, will need to identify the most appropriate regime, tailored to address individual country risks. Therefore, the Guidance does not attempt to provide a single model for the risk-based approach, but seeks to provide guidance for a broad framework based on high level principles and procedures that countries may wish to consider when applying the risk-based approach with the understanding that this guidance does not override the purview of national authorities.

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

The purpose of the Risk-Based Approach

14. The FATF Recommendations contain language that permits countries, in line with the requirements of the FATF Standards, to adopt a risk-based approach to combating money laundering and terrorist financing. That language also authorises countries to permit MSBs to use a risk-based approach to discharging certain of their anti-money laundering (AML) and counter-terrorist financing (CFT) obligations. By adopting a risk-based approach, competent authorities and MSBs are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to 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, so that all MSBs, customers, products, etc. receive equal attention, or that resources are targeted, but on the basis of factors other than the risk assessed. This can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing. Eventually, it is of utmost importance that a risk based approach remains dynamic to risk; able to evolve to match a changed threat, and therefore flexible. MSBs should be able to show how their strategy and approach meet the changing threats as identified by their own staff or external public sector parties.

15. Adopting a risk-based approach implies the adoption of a risk management process for dealing with money laundering and terrorist financing. This process encompasses recognising the existence of the risk(s), undertaking an assessment of the risk(s) and developing strategies to manage and mitigate the identified risks.

16. A risk analysis must be performed, and kept up to date, 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. MSBs will need 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.

17. The strategies to manage and mitigate the identified money laundering and terrorist financing risks in MSBs are typically aimed at preventing the activity from occurring through a mixture of deterrence (*e.g.* appropriate CDD measures in the circumstances stated in paragraph 48), detection (*e.g.* monitoring and suspicious transaction reporting), and record-keeping so as to facilitate investigations.

18. Proportionate procedures should be designed based on assessed risk. Higher risk areas should be subject to enhanced measures for MSBs. This may include the measures mentioned in paragraph 116. It also follows that in instances where risks are low, simplified or reduced controls may be applied.

19. 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 categorizing money laundering risks and establishing reasonable controls based on risks identified. An effective risk-based approach will allow MSBs to exercise reasonable business judgement with respect to their customers. Application of a reasoned and well-articulated risk-based approach will justify the determinations of MSBs with regard to managing potential money laundering and terrorist financing risks and allow MSBs to exercise reasonable business judgement with respect to their customers. A risk-based approach should not be designed to prohibit MSBs from engaging in transactions with customers or

establishing relationships with potential customers, but rather it should assist MSBs to effectively manage potential money laundering and terrorist financing risks.

20. Regardless of the strength and effectiveness of AML/CFT controls established by MSBs, criminals will continue to attempt to move illicit funds through the financial sector undetected and will, from time to time, succeed. 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 recognized that any reasonably applied controls, including controls implemented as a result of a reasonably implemented risk-based approach will not identify and detect all instances of money laundering or terrorist financing. Therefore, regulators, law enforcement and judicial authorities must take into account and give due consideration to a MSB's well-reasoned risk-based approach. When MSBs do not effectively mitigate the risks due to a failure to implement an adequate risk-based approach or failure of a risk-based programme that was not adequate in its design, regulators, law enforcement or judicial authorities should take necessary action, including imposing penalties, or other appropriate enforcement/regulatory remedies.

Potential Benefits and Challenges of the Risk-Based Approach

Benefits:

21. 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 MSBs and supervisory authorities to be more efficient and effective in their use of resources and minimise burdens on customers. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively.

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

23. Money laundering and terrorist financing risks can be more effectively managed through a risk-based process that assesses all potential risks, and which is built on a true cooperative arrangement between competent authorities and MSBs. Without cooperation and understanding between these parties, there can be no effective risk-based process.

24. Money launderers and terrorist organisations have considerable knowledge of the financial sector and take extreme measures to hide their financial activities and make them indistinguishable from legitimate transactions. A risk-based approach is designed to make it more difficult for these criminal elements to make use of MSBs due to the increased focus on the identified higher risk activities that are being undertaken by these criminal elements. In addition, a risk-based approach allows MSBs to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

Challenges:

25. A risk-based approach is not necessarily an easy option, and there may be barriers 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 41 to 45 below.

26. 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 judgment be exercised in the implementation within the institution and its subcomponents of such 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 to perform a transaction.

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

28. MSBs may find that some staff members are uncomfortable making risk-based judgments. 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 recognize or underestimates the risks, a culture may develop within the business that allows for inadequate resources to be devoted to compliance leading to potentially significant compliance failures. Supervisors should place greater emphasis on whether the MSBs have an effective decision-making process. However, sample testing should be used or individual decisions reviewed as a means to test the effectiveness of the business's overall risk management (see paragraph 88). Supervisors should appreciate that even though the MSB has established appropriate risk management structures and procedures that are regularly updated, and has followed the relevant policies, procedures, and processes, the MSB may still make decisions that were incorrect in light of additional information not reasonably available at the time.

29. In implementing the risk-based approach MSBs should be given the opportunity to make reasonable judgments. This will mean that no two businesses are likely to adopt the exact same detailed practices. Such potential diversity of practice will require that regulators make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges to supervisory staff working to monitor compliance. The existence of good practice guidance, supervisory training, industry studies and other available information and materials will assist supervisors in determining whether a MSB has made sound risk-based judgments.

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

Potential Benefits:

- Better management of risks and cost-benefits.
- Money service business focuses 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 judgments.
- Regulatory response to potential diversity of practice.

Chapter Three: FATF and the Risk-Based Approach

30. The varying degrees of risk of money laundering or terrorist financing for particular types of MSBs or for particular types of customers, products or transactions is an important consideration underlying the FATF Recommendations. According to the Recommendations countries may take risk into account in two ways: (a) there is a general risk principle that applies to MSBs, and which allows countries in some cases to choose not to apply certain Recommendations either partially or fully, provided certain conditions are met; and (b) 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). In all cases, when assessing risk, due regard should be given to the attractiveness to criminals and terrorists of using channels which they identify as suiting their purpose. Low risk channels can sometimes become the target for 'misuse' too.

General Risk Principle

31. A country could decide that it will apply the full range of AML/CFT measures set out in Recommendations 5-11, 13-15, 18 and 21-22, to all types of financial institutions[1]. However, that country may also decide to take risk into account, and may decide to limit the application of certain Recommendations provided that either of the conditions set out below are met. Where there are limitations or exemptions, this should be done on a strictly limited and justified basis:

- When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing[2] activity occurring, a country may decide that the application of AML measures is not necessary, either fully or partially.

- In strictly limited and justified circumstances, and based on a proven low risk of money laundering or terrorist financing, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities.

Specific Risk References

32. In addition to the general risk principle referred to above, 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 institutions, businesses and professions covered by the FATF Recommendations, risk is addressed in four principal areas: (a) Customer Due Diligence measures (R.5-9); (b) institutions' internal control systems (R.15 & 22); (c) the approach to regulation and oversight by competent authorities (R.23); and (d) provision for countries to allow Designated Non-Financial Businesses and Professions (DNFBPs) to take the risk of money laundering or terrorist financing into account in a similar way to MSBs (R.12, 16 & 24).

---

1 See *FATF Recommendations Glossary*, definition of "financial institution".

2 The reference to terrorist financing in these two statements was added in the FATF Methodology paragraph 20(a) and (b).

Customer Due Diligence (R.5-9)

33. Risk is referred to in several forms:

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

b) Lower risk – A country may also permit its MSBs to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). MSBs may thus reduce or simplify (but not avoid completely) the required measures. Two possible examples of where there may be lower money laundering/terrorist financing risks include MSBs that are subject to the requirements consistent with the FATF Recommendations and supervised for compliance with those requirements, and listed public companies that are subject to regulatory disclosure requirements.

c) Risk arising from innovation – Under Recommendation 8, a country must require its MSBs 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 competent authorities assess or review the procedures adopted by MSBs to determine the degree of risk and how they manage that risk, as well as to review the determinations made by businesses. This expectation applies to all areas where the risk-based approach applies. In addition, where the competent authorities have issued guidelines to MSBs on a suitable approach to risk-based procedures, it will be important to establish that the MSBs have indeed followed such guidelines. The Recommendations also recognise that country risk is a necessary component of any risk assessment mechanism (R.5 & 9).

MSB's internal control systems (R.15 & 22)

34. 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 businesses 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. Similarly, country risk (and the implementation of the FATF Recommendations) must be taken into account when assessing the measures being undertaken by foreign branches and subsidiaries (R.22).

Regulation and oversight by competent authorities (R.23)

35. Under Recommendation 23, a country may have regard to the risk of money laundering or terrorist financing in a particular financial sector when determining the extent of measures to license or register and appropriately regulate, and to supervise or oversee those businesses for AML/CFT purposes. If there is a proven low risk of money laundering and terrorist financing then lesser measures may be taken. The extent of the measures for persons providing money or value transfer services and money/currency changing services are subject to stated minimum standards.

Designated Non-Financial Businesses and Professions (R.12, 16, 24)

36. In implementing AML/CFT measures for DNFBPs under Recommendations 12 and 16, a country may permit DNFBP's to take money laundering and terrorist financing risk into account when determining the extent of CDD, internal controls etc, in a way similar to that permitted for financial institutions.[3]

37. As regards regulation and monitoring (R.24), a country may have regard to the risk of money laundering or terrorist financing in a particular DNFBP sector (except for casinos which have been determined to be higher risk) when determining the extent of measures required to monitor or ensure compliance for anti-money laundering and counter terrorist financing purposes. If there is a proven low risk of money laundering and terrorist financing then lesser monitoring measures may be taken.[4]

Other Recommendations

38. As regards the FATF Nine Special Recommendations on Terrorist Financing, SR VI aims at increasing the transparency of payment flows by ensuring that jurisdictions impose consistent AML/CFT measures in all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector. SR VI requires jurisdictions to designate one or more competent authorities to register and/or licence natural and legal persons that perform money or value transfer services, including through informal system, to submit these operators to applicable FATF Recommendations and Special Recommendations (in particular R. 4-11, 13-15, 21-23, SRVII) and to require each licenced or registered money / value transfer operators to maintain an updated list of their agents, which must be available to competent authorities. In addition, jurisdictions should be able to impose sanctions in case of failure with the licencing and/or registration requirement and with the relevant FATF Recommendations. As for Recommendation 23, a jurisdiction may have regard to the risk of money laundering or terrorist financing when determining the extent of measures to license or register and appropriately regulate, and to supervise or oversee those businesses for AML/CFT purposes. If there is a proven low risk of money laundering and terrorist financing then lesser measures may be taken. The extent of the measures for persons providing money or value transfer services and money/currency changing services are subject to the above stated minimum standards.

39. SR VIII dealing with non-profit organisations also recognises that the risk of terrorist financing should be taken into account,[5] and that a targeted approach in dealing with the terrorist threat to the non-profit organisation (NPO) sector is essential given the diversity within individual national sectors and the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists. Likewise the best practices document supporting SR IX encourages countries to base their efforts on assessed risk and threat assessments. Risk is also featured in the methodology supporting SR VII, where beneficiary financial institutions should be required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information.

40. Recommendation 25 requires adequate feedback to be provided to the financial sector and DNFBPs. Such feedback helps institutions and businesses to more accurately assess the money laundering and terrorist financing risks and to adjust their risk programmes accordingly. This in turn makes it more likely that better quality suspicious transaction reports will be filed. As well as being an essential input to

---

3 *AML/CFT Evaluations and Assessments - Handbook for Countries and Assessors*, paragraph 43(e) (i)

4 See *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, R.24.

5 *AML/CFT Evaluations and Assessments - Handbook for Countries and Assessors*, paragraph 43 (f).

any assessment of country or sector wide risks, the promptness and content of such feedback is relevant to implementing an effective risk-based approach.

Applicability of the risk-based approach to terrorist financing

41. The application of a risk-based approach to terrorist financing has both similarities and differences compared to money laundering. They both require a process for identifying and assessing risk. However, the characteristics of terrorist financing mean that the risks may be difficult to assess and the implementation 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 come from legal sources.

42. 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 terrorists 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 then it is even more difficult to determine that 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 (*i.e.* commonly held chemicals, a motor vehicle, etc.) to further their goals, with the only covert fact being the intended use of such materials and services purchased. Therefore, both for terrorist funds derived from criminal activity and for legitimately sourced funds, 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 business to determine the type of underlying criminal activity, or intended terrorist purpose, rather the business's role is to 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.

43. Therefore, the ability of MSBs to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or without 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 around 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).

44. Where particular individuals, organisations or countries are the subject of terrorist finance sanctions, the obligations on businesses to comply and the listing of those individuals, organisations or countries as a result of such actions are determined exclusively by countries and are not a function of risk. Violations of such sanctions may result in a criminal offence or sanctions if funds or financial services are made available to a target or its agent.

45. 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. MSBs 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

46. 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.

47. Requirements to freeze assets of identified individuals or entities, in jurisdictions 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.

48. There are a number of components to customer due diligence – identification and verification of identity of customers and beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing due diligence. Of these components, the identification and verification of identity of customers are requirements which must be completed regardless of the risk-based approach for all customers that have an account or a business relationship and when the appropriate monetary thresholds are reached (not higher than USD/EUR 15 000 for occasional transactions or not higher than USD/EUR 1 000 for wire transfers). This is the case for cross-border and domestic transfers of funds between financial institutions, including MSBs. Indeed, Special Recommendation VII requires each country to take measures to require financial institutions, including MSBs, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related messages through the payment chain. However, for domestic wire transfers, the ordering MSB may include full originator information or only the orignator's account number or unique identifier, provided full originator information is available to the beneficiary financial institution and competent authorities within three business days.

49. However, in relation to all the 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 MSBs 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 and purpose of the transaction, 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, whether it is automated, manual, a review of exception reports or a combination of acceptable options, depending on the risks presented, 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 the

customer has begun transacting either through an account or otherwise in the relationship with the MSBs. 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 Supervision and Risk-Based Policies and Processes

52. Risk-based policies and processes in MSBs should be distinguished from risk-based supervision. The methodology adopted by regulatory authorities to determine allocation of supervisory resources should cover the business focus, the risk profile and the internal control environment, and should permit relevant comparisons between MSBs. 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 MSBs are exposed. Consequently, this prioritisation would lead supervisors to demonstrate increased regulatory attention to MSBs that engage in activities assessed to be higher money laundering risks.

53. However, it should also be noted that the risk factors taken into account to prioritise the supervisors' 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.

Summary box:

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

- Money services businesses and regulators 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 recognize that the risk-based approach will not eradicate all elements of risk.
- Authorities have a responsibility to establish an atmosphere in which money services businesses need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Regulators' supervisory staff must be well-trained in the risk-based approach, both as applied by supervisors and by money services businesses.
- Requirements and supervisory oversight at the national level should be consistent among similar industries.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

Chapter One: High-level principles for creating a risk-based approach

54. The creation of a risk-based approach to countering money laundering and the financing of terrorism will allow competent authorities and MSBs 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.

55. 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

56. 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.

57. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of competent authorities and the nature of the financial services sector, 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 document. It should be considered as a process that is designed to achieve a specific outcome. 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. Competent authorities, in consultation with the private sector, should consider how best to achieve this while also taking into account any risk associated with providing information on vulnerabilities in their financial systems to money launderers, terrorist financiers, and other criminals[6].

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

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

59. The risk-based approach does not mean the absence of a clear statement of what is required from MSBs. However under a risk-based approach, MSBs 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 a

[6] See *FATF Report on Money Laundering and Terrorist Financing Risk Assessment Strategies*, adopted in June 2008.

particular MSB. The fact that policies and procedures, in accordance to the risk levels, may be applied flexibly to different products, services, customers and locations does not mean that policies and procedures need not be clearly defined.

60. Basic minimum AML requirements can coexist 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 supervisory framework to support the application of the risk-based approach

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

62. Where appropriate, regulators should seek to adopt a risk-based approach to the supervision of MSBs' controls to combat money laundering and terrorist financing. This should be based on a thorough and comprehensive understanding of the types of financial activity undertaken and the money laundering and terrorist financing risks of those activities. Regulators will probably need to prioritise resources based on their overall assessment of where the risks are, which institutions are most exposed to them, and other factors.

63. Regulators with responsibilities other than those related to AML/CFT will need to consider these risks alongside other risk assessments arising from the regulator's wider duties. Similarly, efforts should be made to ensure appropriate cooperation between competent authorities, which supervise similar activities.

64. Such risk assessments should help the regulator choose where to apply resources in its supervisory programme, with a view to using limited resources to achieve the greatest effect. A risk assessment may also identify that the regulator does not have adequate resources to deal with the risks[7]. In such circumstances the regulator may need to obtain additional resources or adopt other strategies to manage or mitigate any unacceptable residual risks.

65. The application of a risk-based approach to supervision requires that regulators' staff be able to make principle-based decisions in a similar fashion as would be expected from staff of a MSB that has adopted a risk-based approach. These decisions will cover the adequacy of MSB's arrangements to combat money laundering and terrorist financing. As such, a regulator may wish to consider how best to train its staff in the practical application of a risk-based approach to supervision. Supervisory staff will need to be well-briefed as to the general principles of a risk-based approach, its possible methods of application, and what a risk-based approach looks like when successfully applied by MSBs.

Principle Four: Identifying the main actors and ensuring consistency

66. Countries should consider who the main stakeholders are when adopting a risk-based approach to combating money laundering and terrorist financing. These will differ between countries. Thought should be given as to the most effective way to share responsibility between these parties, and how information

[7] See FATF Recommendation 30.

may be shared to best effect. For example, which body or bodies are best placed to provide guidance to MSBs about how to implement a risk-based approach to anti money laundering and counter-terrorist financing.

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

- Government – this may include legislature, executive, and judiciary.
- Law enforcement agencies - this might include the police, customs etc.
- The financial intelligence unit (FIU), security services, other similar agencies etc.
- Financial services regulators.
- The MSB private sector – this might include MSBs companies or professional associations.
- 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 MSB firms.
- Others – those who are in a position to contribute to the conceptual basis underpinning the risk-based approach, such stakeholders may include academia and the media.

68. Clearly a government will be able to exert influence more effectively over some of these stakeholders than others. However, 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.

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

- MSBs 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 MSB's ability to detect and deter money laundering and terrorist financing can sometimes be necessarily limited and that information on risk factors is not always robust or freely available. There should therefore be reasonable policy and supervisory expectations about what a MSB with good controls aimed at preventing money laundering and the finance of terrorism is able to achieve. A MSB 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 will be identical and as a result will not always require precisely the same type of enhanced due diligence.

Principle Five: Information exchange between the public and private sector

70. 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 competent authorities with information they identify as a result of previously provided government intelligence.

71. Public authorities, whether law enforcement agencies, regulators or other bodies, have privileged access to information that may assist MSBs to reach informed judgments when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, MSBs routinely transact with a great number of customers on a daily basis, and are able to understand their customer base. 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.

72. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, supervisors 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.

73. 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.[8] 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 financial system.
- Feedback on suspicious transaction reports and other relevant reports.
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards, it may also be appropriate for authorities to share targeted confidential information with MSBs.
- Countries, persons or organisations whose assets or transactions should be frozen.

74. When choosing what information can be properly and profitably shared, public authorities may wish to emphasize to the financial services industry that information from public bodies should inform, but not be a substitute for institutions' own judgments. For example, countries may decide to not 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 MSBs' decision making processes, along with any other relevant information that is available to the MSBs.

8 Examples of such dialogue are included in annex 1 of these guidelines.

Chapter Two: Implementation of the Risk-Based Approach

Assessment of Risk to Inform National Priorities

75. 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 scale, whether by countries or individual MSBs. 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'.

76. A national risk assessment should be regarded as a description of fundamental background information to assist supervisors, law enforcement authorities, and the FIU 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.

77. 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 of the financial services industry.
- Composition of the financial services industry.
- Ownership structure of MSBs.
- The scale and type of business done by unregistered or unlicensed MSBs.
- Corporate governance arrangements in MSBs and the wider economy.
- The nature of payment systems and the prevalence of cash-based transactions.
- Geographical spread of financial industry's operations and customers.
- Types of products and services offered by the financial services industry.
- Types of customers serviced by the financial services industry.
- 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 areas in the economy.

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

79. 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, competent authorities should develop and implement measures to mitigate the identified risks.

80. 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. Countries, in partnership with law enforcement bodies, FIUs, and regulators, 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: they 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.

81. 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 how those bodies make use of their resources in an effective manner.

82. As well as assisting competent authorities to decide how to allocate public funds to combat money laundering and terrorist financing, a national risk assessment can also inform decision-makers about the relationship between the supervisory/regulatory regime and the identified risks. An over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on industry, and act against the interests of the public by limiting access to financial services for some segments of the population. Alternatively, efforts may not be sufficient to provide protection to societies from the threats posed by criminals and terrorists. A sound understanding of the risks at the national level could help obviate these dangers.

Regulatory Supervision – General Principles

Defining the acceptable level of risk

83. 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 factors.

84. As described in Section One, all financial activity involves an element of risk. Competent authorities should not prohibit MSBs 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 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 financial services.

85. However, this does not exclude the need to implement basic minimum requirements. For instance FATF Recommendation 5 states that *"*Where the financial institution 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.

86. Competent authorities expect MSBs 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 MSBs 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.

87. 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, supervisors will expect MSBs to identify individual high risk categories and apply specific and appropriate mitigation measures. For example, some categories could be:

- Non-resident customers (to understand why they want to enter in business relationship in a different country).
- Politically exposed persons (to apply a specific policy).
- Companies with bearer shares (to exert particular vigilance on the identification and verification of the beneficial owner).
- Further information on the identification of specific risk categories is provided in Section Three, "Guidance for the Private Sector".

Proportionate Supervisory Actions to support the Risk-Based Approach

88. Supervisors should seek to identify weaknesses through an effective programme of both on-site and off-site supervision[9], and through analysis of internal and other available information.

89. In the course of their examinations, supervisors should review a MSB'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 the business and the adequacy of its mitigation measures. Where available, assessments carried out by or for the business may be a useful source of information. The assessment should include sample transaction testing of customer transactions to validate the assessment. The supervisor's assessment of management's ability and willingness to take necessary corrective action is also a critical determining factor. Supervisors should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe supervisory response.

90. 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, transaction monitoring, staff training and internal controls, and therefore, might alone justify supervisory action.

91. Supervisors should be in a position to compare risk factors and procedures used by peer MSBs. This will, among other objectives, assist the supervisors in better understanding how MSBs are developing and implementing a risk-based approach, as well as in identifying potential deficiencies. Similarly, supervisors can and should use their knowledge of the risks associated with products, services, customers and geographic locations to help them evaluate the MSB's money laundering and terrorist financing risk assessment, with the understanding, however, that they may possess information that has not been made available to MSBs and, therefore, MSBs would not have been able to take such information into account when developing and implementing a risk-based approach. Supervisors (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist MSBs in managing their risks. Where MSBs are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by the competent authorities[10]. An assessment of the risk-based approach will, for instance, help identify cases where businesses 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.

92. In the context of the risk-based approach, the primary focus for supervisors should be to determine whether or not the MSB'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 supervisory goal is not to prohibit high risk activity, but rather to be confident that MSBs have adequately and effectively implemented appropriate risk mitigation strategies.

93. Under FATF Recommendation 29, supervisors should impose adequate sanctions for failure to comply with statutory and regulatory requirements to combat money laundering and terrorist financing, and effective AML/CFT supervision requires that the supervisor has available an appropriate range of

---

9 FATF *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, criteria 29.2.

10 FATF Recommendations 5 & 25, *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, Essential Criteria 25.1 and 5.12.

supervisory tools for use when, in the supervisor's judgement, a financial institution is not complying with laws, regulations or supervisory decision. These tools include the ability to require a MSB to take prompt remedial action and to impose penalties. In practice, the range of tools is applied in accordance with the gravity of a situation.

94. Fines and/or penalties are not appropriate in all regulatory actions to correct or remedy AML/CFT deficiencies. However, supervisors must have the authority and willingness to apply fines and/or penalties in cases where substantial deficiencies exist. More often than not, action should take the form of a remedial program through the normal supervisory processes.

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

a) Regulatory Transparency

96. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Supervisors are aware that MSBs, while looking for operational freedom to make their own risk judgments, will also seek guidance on regulatory obligations. As such, the regulator with AML/CFT supervisory responsibilities should seek to be transparent in setting out what it expects from regulated institutions, 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 process.

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

b) Staff Training of Supervisors and Enforcement Staff

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

99. Training should aim to allow supervisory staff to form sound comparative judgements about MSBs AML/CFT systems and controls. It is important in conducting assessments that supervisors have the ability to make judgements regarding management controls in light of the risks assumed by businesses and considering available industry practices. Supervisors might also find it useful to undertake comparative assessments so as to form judgements as to the relative strengths and weaknesses of different businesses' arrangements.

100. The training should include instructing supervisors about how to evaluate whether senior management have implemented adequate risk management measures, and that the necessary procedures and controls are in place. The training should also include reference to specific guidance, where available. It should be noted that "the supervisory process should include not only a review of policies and procedures, but also a review of customer files and the sampling of some accounts"[11]. The supervisor has equally to assess whether or not the processes are adequate, and if it determines that the risk management processes are inadequate, it has the power to require a business group to strengthen them. Supervisors also

[11] See FATF Recommendations, R.29.

should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

101. To fulfil these responsibilities, training should enable supervisory 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 the MSB's 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.

Whilst by no means an exhaustive list, onsite examination topics may include the following:

- The application of a group-wide policy.
- Assessment of the risk associated with each business line.
- The extent that assessments have been formally documented and segmented by products, delivery channels, types of customer and geographic location of customers.
- Extent of CDD procedures including identification of new customers, customer profiling and collection of 'Know Your Customer' information.
- Additional due diligence is undertaken in relation to high risk customers and businesses, *e.g.* 'high net worth' individuals, Politically Exposed Persons.
- Transaction monitoring procedures in place and how alerts are reviewed.
- Policies determining how and on what basis existing customer files may be updated.
- Quality of internal systems and controls, including processes for identifying and reporting large cash and suspicious transactions.
- Policies on record keeping and ease of retrieving identification evidence or transaction records.
- Scope, frequency and audience of AML/CFT training and evaluation of effectiveness.
- Appropriate sample testing.

There is no set of 'right answers' to these topics. The key considerations are that (a) the money services business is meeting any minimum regulatory requirements (b) the money services business has identified its money laundering and terrorist financing risks, worked out how best to manage those risks, and devoted adequate resources to the task; and (c) senior management is properly accountable for AML/CFT controls.

SECTION THREE: GUIDANCE FOR MONEY SERVICES BUSINESSES ON IMPLEMENTING A RISK-BASED APPROACH

Preamble

102. The specifics of a MSB's particular risk-based process to manage and mitigate its ML/TF risks should be determined based on the operations of the business, including its size, the products and services offered, and its geographic scope of operations. Where appropriate and feasible the policies and procedures setting out how a MSB will manage and mitigate its money laundering and terrorist financing risks should be articulated on a company or group-wide basis. However, it is noted that the characteristics of terrorist financing present differently from money laundering and, therefore, the associated risk may be difficult to assess without a more comprehensive set of indicators of the methods and techniques used for terrorist financing (see paragraphs 40 to 44). Because there are no clear red flags for detecting activity related to terrorist financing, and because terrorist financing methods can be the same or similar to money laundering, the identification of terrorist financing itself can be a difficult process. A reasonably designed risk-based approach provides the means by which a MSB identifies the criteria to assess potential money laundering/terrorist financing (ML/TF) risks. Whenever integrated in a group, the MSB should be fully integrated and apply a consistent risk-based approach to all their operations. No obstacle should hinder communication of information among the different agents of the group, and there should also be testing compliance with group-wide policies. Such compliance tests could usefully also be reviewed by external auditors and supervisors. One component of a reasonably designed risk-based approach is a geographic risk assessment, which can aid in identifying geographic locations that may pose a higher risk, such as countries subject to government sanctions. A reasonably implemented risk-based process provides a framework for identifying the degree of potential ML/TF risks associated with customers and transactions and allows the business to focus on those customers and transactions that potentially pose the greatest risk of ML/TF. To further combat the threat of the MSB's systems being used for terrorist financing, customer transactions should be screened against applicable government lists.

103. Depending upon the jurisdiction and the licensing/registration structure, the MSB sector can be regulated as a financial institution that offers similar services. MSBs are required to monitor and report suspicious activity and, if required by domestic law, large transactions, collect required customer identification at specific monetary thresholds, and maintain certain records in accordance with applicable regulations. This guidance focuses on the transfer of money or value and the money and currency changing operated by MSBs. In some cases, MSBs maintain account relationships with customers. In most cases, MSBs operate in a transaction-based environment.

104. Performing a risk assessment is the foundation of a risk-based approach. The intent of a risk assessment is to identify products, services, geographic locations and points of customer interaction that are most susceptible to ML/TF activities. The risk assessment also serves to highlight remaining areas of exposure that should be addressed after applying a regime of risk-based internal controls. A risk assessment may include a variety of factors, depending upon the particular circumstances, including but not limited to:

- The nature, scale and complexity of the business's operations, including geographical diversity.

- The initial and ongoing due diligence or monitoring conducted on the business's agent locations.
- The business's customer, product, and activity profile.
- The nature of the business relationship (*i.e.* occasional vs. ongoing relationship).
- The distribution channels used.
- The electronic systems or platform used for data transmission.
- The transaction monitoring being performed.
- The volume and size of transactions.
- The extent to which the business is dealing directly with customers or is dealing through intermediaries, third parties or in a non-face-to-face setting.

105. To conduct a proper risk-based approach, MSBs need to collect information. The effectiveness of the risk-based approach would increase significantly if MSBs could share information with other MSBs without any form of legal impediments with the other parties of a transaction, whether they are both part of a financial group or not, and in particular if the other MSB is located in a foreign country.

Chapter One: Risk Categories

106. In order to implement a risk-based approach, MSBs should identify the criteria to assess potential ML/TF risks. Identification of the ML/TF risks, to the extent that such risks can be identified, of customers or categories of customers, products, services, geographic areas, and transactions will allow MSBs to determine and implement proportionate measures and controls to mitigate these risks. Regarding the risk assessment of a class or type of customer, it is worth noting that while it should always be performed at the inception of a customer relationship, for some customers, risk factors may only become evident once the customer has begun transacting, making monitoring of customer transactions and on-going reviews a fundamental component of a reasonably designed risk-based approach. A MSB may also have to adjust its risk assessment based on information received from competent authorities.

107. ML/TF risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling MSBs to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer risk; and product/service risk. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary from one institution to another, depending on their respective circumstances. Consequently, MSBs will have to make their own determination as to the risk weights; however, parameters set by law or regulation may limit a business's discretion.

108. While there is no agreed upon set of risk categories, the examples provided herein are the most commonly identified risk categories. There is no one single methodology to apply to these risk categories, and the application of these risk categories is intended to provide a strategy for managing the potential risks.

Country/Geographic Risk

109. There is no universally agreed upon definition, by either competent authorities or by MSBs, that prescribes whether a particular country or geographic area (including the country/area within which the MSB operates) represents a higher risk. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may result in a determination that a country poses a higher risk include:

- Countries identified by FATF Statements as having a weak AML/CFT regime, and for which financial institutions should give special attention to business relationships and transactions.

- 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 recognized, may be given credence by the MSB because of the standing of the issuer and the nature of the measures.

- Countries/areas identified by credible sources[12] as lacking appropriate AML/CFT laws, regulations and other measures.

[12] "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, the World Bank 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

- Countries/areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

- Countries/areas identified by credible sources as having significant levels of corruption, or other criminal activity, including source or transit countries/areas for ongoing criminal activity, such as illegal drugs, human trafficking and smuggling, systematic frauds and illegal gambling.

110. Depending on the products or services offered, a MSB should consider the geographic risk involved in the transaction conducted. This may include but is not limited to the following:

- A money transfer sent to or received from a high-risk jurisdiction/area.

- A customer completing a currency exchange transaction then sending money to a high-risk jurisdiction.

Customer Risk

111. Determining the potential ML/TF risks, to the extent that terrorist financing risk can be identified, is critical to the development of an overall risk framework. Based on its own criteria, a MSB should determine whether a particular customer poses 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:

- Customer conducting their business relationship or transactions in unusual circumstances, such as:

  – Customer who travels unexplained distances to locations to conduct transactions.

  – Transfer with no apparent business or lawful purpose.

  – Unusual single or multiple-day activity.

  – Higher volume or frequency of transactions sent or received with no logical or apparent purpose.

  – Customer networks; *i.e.* defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.

  – Customer offers a bribe or offers a tip other than where a tip is customary.

- Customer who is a Politically Exposed Person.

- Non face-to-face customer.

- Customer structures their transaction (breaks up amounts to avoid reporting or record keeping).

- Customer wires money to online gambling sites.

---

regulation and should not be viewed as an automatic determination that something is of higher risk, but it provides a very important indicator of the degree of geographic risk.

- Customer wires money to high-risk jurisdictions.
- Customer who uses agents or associates where the nature of the relationship or transaction(s) make it difficult to identify the beneficial owner of the funds.
- Customer knows little or is reluctant to disclose details about the payee (address/contact info, etc).
- Customer or party involved in the transaction have no apparent ties to the destination country.
- Suspicion that the customer is acting on behalf of a third party but not disclosing that information.
- Transaction involving certain charities and other not-for-profit organizations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis).
- Customer who has been the subject of a law enforcement inquiry known by the MSB.
- Customer who offers false identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g., use of identification cards issued by different countries).
- Customer who offers different identifications or different identifiers (such as phone or address) on different occasions.
- Customer who receives transactions in a pattern consistent with criminal proceeds, *e.g.* from elderly people in a wide geographic area, in amounts consistent with a lottery scam.
- Customer who receives transfers in seasonal patterns consistent with criminal proceeds; *e.g.* marijuana growing season, illegal immigration.

Product / Transaction / Service Risk

112. An overall risk assessment should also include determining the potential risks presented by products and services offered by a MSB. A MSB should be mindful of the risks associated with new or innovative products or services not specifically offered by the MSB, but that make use of the MSB's systems to deliver the product or service. Determining the risks of products and services should include a consideration of such factors as:

- Products or services that may inherently favour a degree of anonymity or can readily cross international borders, such as online money transfers, stored value cards, money orders and money transfers by mobile phone.
- Products or services that have a very high or no transaction limit.
- The global reach of the product or service offered.
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

113. The risk associated with the transaction may vary depending on whether the MSB is sending or receiving the transaction. An overall risk assessment should include a review of transactions as a whole. This should include a consideration of such factors as:

a) Transactions sent:

- Customer behaviours at point of origination:
  - Transaction is unnecessarily complex for its stated purpose.
  - Transfers being made on behalf of a third party.
  - Transaction is inconsistent with financial standing or occupation, or is outside the normal course of business for the customer in light of the information provided by the customer when conducting the transaction or during subsequent contact (such as an interview) with the customer.
  - Customer is willing to pay unusual fees to have transactions conducted.
  - Customer has vague knowledge about amount of money involved in the transaction.
  - Customer is clearly blind to the fact that the transaction seems to involve ML/TF.
  - Customer makes inquiries or tries to convince staff to avoid reporting.
  - Customer sends money internationally and then says expects to receive an equal incoming transfer.
  - Customer receives a wire transfer and immediately sends an equal money transfer.
  - Unusually large wire transfers.
  - Customer sends frequent wire transfers to foreign countries but does not seem to have any connection to the destination countries.
  - Unusual currency exchange (*e.g.* small denomination currency for high denomination currency).
- Activity detected during back-end monitoring:
  - Transfers to the same person from different individuals or to different persons from the same individual.
  - Customer receives a wire transfer and immediately sends an equal money transfer.
  - Unusually large aggregate wire transfers.
  - Customer uses aliases and a variety of similar but different addresses.
  - A network of customers using a shared address.

In many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and during back-end transaction monitoring.

b) Transactions received:

- The domestic wire transfers received by an MSB company of EUR/USD 1 000 or more should be accompanied, within the message or payment form, by the originator's account number or a unique identification number. Cross-border wire transfers of EUR/USD 1 000 or more should include full originator information (name of the originator, the originator's account number or a unique reference number, the originator's address or national identity number or customer identification number or date and place of birth). Therefore MSBs should pay special attention:
  - To transactions that are not accompanied by the complete originator information required.
  - When additional information has been requested to an ordering MSB, but is still lacking.
- Customer receives transactions in a pattern consistent with criminal proceeds, *e.g.* from elderly people in a wide geographic area, in amounts consistent with a lottery scam.
- Customer receives transfers in seasonal patterns consistent with criminal proceeds; *e.g.* marijuana growing season, illegal immigration.
- Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual needs or receiving pattern.

Agents Risk

114. An overall risk assessment should analyze specific factors which arise from the use of certain agents[13] to facilitate the delivery of MSBs products and services. In some cases these agents may also use the products and services themselves. Assessing agent risk is more complex for those MSBs with an international presence due to varying jurisdictional requirements and the logistics of agent oversight. This agent risk analysis should include such factors as the following based on the reasonableness and appropriateness of the factor within the MSB's business model, systems and controls:

- Agents conducting an usually high number of transactions with another agent location, particularly with an agent in a geographic area of concern.
- The transaction volume of the agent, either overall or relative to typical past transaction volume.
- Agents that have been referred by other departments of the MSB.
- Agents that have been the subject of negative attention from credible media or law enforcement inquiries.
- Agents that are not in compliance with internal policies and external regulation, such as compliance programme requirements, monitoring, reporting, or Know Your Customer practices.

[13] FATF Glossary gives the following definition to agent: "for the purpose of SRVI, an agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licencees, franchisees, concessionaires).

- Agents that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination.

- Agents who fail to provide required originator information upon request.

- Agents whose data collection is lax, sloppy or inconsistent.

- Agents willing to accept false identification.

- Agents willing to enter identification into records that contains false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers.

- Agents with a send-to-receive ratio that is not consistent with other agents in the locale or is consistent with participation in a criminal transaction corridor.

- Agents whose seasonal business fluctuation is not consistent with other agents in the locale or is consistent with participation in a criminal transaction corridor.

- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations.

- Agents whose ratio of questionable or anomalous transactions to transactions that are not in such sets is out of the norm for comparable locations.

Variables That May Impact Risk

115. A MSB's risk-based approach methodology may take into account risk variables specific to certain categories of customers or transactions. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include:

- The purpose of the transaction: transactions conducted primarily to facilitate traditional, low denominated consumer transactions may pose a lower risk than transactions conducted to facilitate the movement of large quantities of cash.

- The type of transaction: a transaction sent by an individual for a commercial bill payment may pose a lower risk than a retail transaction conducted between two individuals.

- The method of sending or receiving the transaction: a non face-to-face transaction may pose a higher risk than a transaction conducted in a face-to-face environment.

- The type of customer: a walk-in customer may pose a higher risk than a known customer with established transaction history and a long-standing relationship with the MSB and/or the agent location.

- The level of cooperation from the customer when asked to provide personal information relating to the nature of the transaction: customers who are forthcoming and readily provide credible information regarding the nature of the transaction when asked may pose a lower risk than customers who become irate or defensive or are unaware of information that they would be expected to know in the circumstances as they present them (such as the phone number of the person to whom they are sending thousands of dollars).

- The rate of recurrence in which an MSB receives a request for a specific type of transaction: transaction types that are requested and seen less frequently may pose a higher risk than transaction types conducted on a regular basis. Transactions that are out of the norm in light of the information provided by the customer at the time of the transaction should be considered higher risk.

Controls for Higher Risk Situations

116. MSBs should implement appropriate measures and controls to mitigate the potential ML/TF risks of those situations that are considered to be higher risk as the result of the MSB's risk assessment. These measures and controls may include:

- Increased levels of know your customer (KYC) or enhanced due diligence, such as proactive contact with the customer to determine the reason for the transactions, the customer's relationship to the sender or receiver, and the source of funds.

- Increased levels of controls and frequency of reviews of customer relationships.

- Increased transaction monitoring of higher-risk products, services and channels.

- Increased awareness by the business of higher-risk customers and transactions.

- Enhanced systematic controls and data integrity at the points of payment, particularly at higher risk agent location.

- Aggregation of activity by a known or a new customer.

- The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that a business establish specific controls targeting each and every risk criteria.

Chapter Two: Application of a Risk-Based Approach

Customer Due Diligence/Know Your Customer

117. Customer Due Diligence (CDD) or Know Your Customer (KYC) processes are intended to enable a MSB to form a reasonable belief that it knows the true identity of each customer at the time the customer conducts the transaction or during a back-end review of the customer's pattern of activity. The CDD or KYC processes for a MSB differ from those of a financial institution such as a bank or securities firm, in that a MSB typically provides occasional, transaction-based services to walk-in customers and generally does not open or maintain accounts. However, MSBs sometimes also introduce customer loyalty schemes and relationship management tools like membership cards. The MSB's CDD or KYC processes are largely tied to its ability to monitor and analyze transaction activity after the activity has occurred. The MSB should have procedures, which are effectively implemented and used to:

a) Identify and verify the identity (a) of each customer conducting or attempting to conduct a transaction at or above the legal monetary thresholds[14]; (b) of each customer that has an ongoing business relationship involving multiple transactions over a period of time with a MSB, by physical examination of the customer's identification document(s) at the time the transaction is being conducted or the business relationship is being established, and

b) When the transaction is a wire transfer[15] higher than EUR/USD 1 000, the identity of the customer should include the following information, referred as "full originator's information": name, customer's account number or unique reference number, and customer's address or national identity number, or customer's identification number, or date and place of birth, and this information should be included in the message or the payment form accompanying the wire transfer. For domestic wire transfers, the ordering MSB may include full originator information or only the orignator's account number or unique identifier provided that full originator information is available to the beneficiary financial institution and competent authorities within 3 business days.

c) In the circumstances described in a) or b), MSBs should also:

---

14 The FATF requires that any national threshold is no higher than USD/EUR 15 000 for occasional transactions (other than wire transfers), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked. See Interpretive Note to Recommendations 5, 12 and 16.
For cross-border wire transfers exceeding USD/EUR 1 000, the originating institution should include 'full originator information,' which includes: the originator's name and account number where an account exists, or in the absence of an account, unique reference number; either the originator's address or national identity number, customer identification number, or date and place of birth. In the case of a domestic wire transfer exceeding the above threshold, if full originator information can be made available to the receiving financial institution and appropriate authorities by other means, the originating institution need only include the name and account number or unique identifier. See Interpretive Note to SR VII. It is noted that in some countries or jurisdictions the obligations to include originator information in funds transfers may apply irrespective of any threshold.

15 The term wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

- 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.

- For higher risk transactions or customer, obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions. If appropriate, obtain appropriate additional subsequent information to understand the customer's circumstances, including the relationship to the sender or receiver, and the source of funds.

- Periodically update relevant CDD information together with the customer risk assessment.

- If appropriate and practical during a back-end review of the customer's activity, obtain appropriate additional subsequent information to understand the customer's circumstances, including the nature of the transaction, the relationship to the sender or receiver, and the source of funds.

118. The starting point is for a MSB to assess the risks that certain categories or types of customers may pose taking into consideration any appropriate risk variables before making a final determination. To this end, MSBs can also take into consideration useful examples for higher or lower risks that may be issued by domestic regulators. MSBs will determine the due diligence requirements appropriate to each customer. This may include:

- A standard level of due diligence applied to all customers, specifically, applicable customer identification at appropriate monetary thresholds as required by law, regulation and other national requirements or internal policy and applicable regulations.

- The standard level being reduced in recognized lower risk scenarios, such as conducting transactions for:

  – Publicly listed companies subject to regulatory disclosure requirements.

  – Other financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations.

- An increased level of due diligence should be applied to those customers determined to be higher risk, such as:

  – Non face-to-face customers.

  – Customers conducting large cash transactions, either carried out in a single operation or in several operations that appear to be linked.

  – Customers conducting higher principal or higher frequency activity.

  – Customers sending to or receiving from higher-risk jurisdictions.

  – Customers located in a higher-risk jurisdiction.

  – Customers who are PEPs.

– Customer circumstances are as described in paragraph 111 above.

Monitoring of Customers and Transactions

119. The degree and nature of monitoring by a MSB will depend on the size of the MSB, the AML/CFT risks that the business has, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, MSBs and their regulatory supervisors must recognize that not all transactions, accounts 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 nature of the transactions. Monitoring methodologies and processes also need to take into account the resources of the MSB. For example smaller MSBs need not implement technologically sophisticated transactions monitoring systems, so long as the methods utilised to conduct monitoring adequately reflect the risk of the MSBs's business.

120. The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each MSB's analysis of its major risks. Regulatory authorities should, therefore, be mindful of and give due weight to the determinations made by MSBs, provided that these determinations are consistent with any legislative or regulatory requirements, and are reasonable and adequately documented.

121. Monitoring under a risk-based approach allows a MSB to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MSBs should also assess the adequacy and integrity of any systems and processes on a periodic basis. The results of the monitoring should be documented, either systematically or manually (or a combination) in order to create a comprehensive audit trail, and maintained according to applicable recordkeeping requirements.

122. National law should provide that for all wire transfers of EUR/USD 1 000 or more, the beneficiary institution should adopt an effective risk-based approach procedure for identifying and handling wire transfers that are not accompanied by full originator information. The lack of full originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or another competent authority.

Suspicious Transaction Reporting

123. The reporting of suspicious transactions or activity is critical to a country's ability to utilize financial information to combat ML/TF and other financial crimes. Countries' reporting regimes are laid down in national law, requiring institutions to file reports when the level of suspicion is reached.

124. When a suspicious transaction report must be made, a risk-based approach is not applicable. However, challenges arise for those MSBs located in multiple jurisdictions. In order to avoid regulatory sanctions, careful attention should be given to proper format, timely filing, and applicable record keeping requirements, since jurisdictional requirements may vary.

125. A risk-based approach is, however, appropriate for the purpose of identifying suspicious activity, for example, by directing additional resources to those areas a MSB has identified as higher risk, such as certain products or services or agents or certain patterns of transaction activity. As part of a risk-based approach, it is also likely that a MSB will utilize information provided by competent authorities to inform its approach for identifying suspicious activity. A MSB should also periodically assess the adequacy and integrity of its system for identifying and reporting suspicious transactions. The decisions for reporting or

not reporting the suspicious activity should be documented, either systematically or manually (or a combination) in order to create a comprehensive audit trail, and maintained according to applicable record keeping requirements.

Training and Awareness

126. Recommendation 15 requires that MSBs provide their employees with AML/CFT training, and it is important that MSBs employees receive appropriate and proportional training with regard to ML/TF. A MSB's commitment to having and maintaining 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.

127. Applying a risk-based approach to the various methods available for training gives each MSB additional flexibility regarding the frequency, delivery mechanisms and focus of such training. Training should be documented and reflect the names of attendees, the dates of attendance, the method of delivery, and the content. Training records should be maintained according to applicable record keeping requirements. A MSB should review its workforce and available resources and implement training programmes that provide appropriate AML/CFT information that is:

- Tailored to the appropriate staff responsibility (*e.g.* management, front-line personnel with direct customer contact, or operations).
- At the appropriate level of detail (*e.g.* front-line personnel, complicated products or customer-managed products).
- At a frequency related to the risk level of the business line involved and to account for staff turnover and agent risk level.
- Provided initially to new staff, and at subsequent periodic intervals to existing staff, in order to reinforce current AML/CFT concerns and introduce new ones.
- Followed by testing to assess and ensure that staff knowledge is commensurate with the detail of information provided.

128. Depending upon regulatory requirements and/or internal policies, including the requirements of its AML compliance programme or industry best practices, a MSB must also require its agents to receive appropriate AML/CFT training. Agent training, too, may be risk-based, but generally may include onsite or offsite initial training (*i.e.* upon activation), and ongoing training via web-based programmes, periodic mailings or newsletters, password-protected informational websites or pop-up messages at point of origination. This training should inform them of any new developments, including information on current ML and FT techniques, methods and trends, and should also clearly inform them about all aspects of AML/CFT laws and obligations. In conjunction with or in addition to such training, the MSB may provide periodic compliance program reviews involving a comprehensive assessment of the agent's compliance with internal and external AML/CFT regulatory requirements.

Agent Due Diligence / Know Your Agent

129. Agent Due Diligence/Know Your Agent is intended to enable a MSB to form a reasonable belief that it knows the legal and ownership structure of its Agent relationships and that it will be forming business relationships with legitimate and viable agents that will reliably implement or adhere to

(depending on local regulations) AML/CFT requirements, program responsibilities, policies, and procedures. The MSB's procedures should consider such factors as:

- Upon application, identify the agent and perform the necessary background checks and due diligence, such as a recent change from another product/service provider, length of time in business, ownership structure, creditworthiness, financial viability, class of trade or industry, licensing and regulatory structure and other regulatory licensing or registration to which the MSB may be subject (*e.g.* as a cheque casher).

- Obtain appropriate additional information to understand the applicant's business, such as offering other MSB services, Agent's past record of legal and regulatory compliance, expected nature and level of transactions and customer base, and geographical exposure.

- Upon approval, conduct new agent AML/CFT training encompassing applicable AML/CFT requirements, AML Compliance program responsibilities, and MSB internal policies and procedures.

- Provide AML/CFT compliance materials, tools, and training to agents on an ongoing, periodic basis.

- Utilize a baseline risk assessment tool that monitors agent activity to measure transaction-related risk or identify agents that exhibit risk behaviours, such as structured transactions, customer identification sharing or biographical information sharing, higher volume senders or payees, unusual and unexplained spikes, ratios or seasonal fluctuations in transaction volume, inferior data quality entered at point of origination or payment, related or poor quality of STR/SAR activity, higher volume agent-to-agent corridors, unusual agent patterns, or unusual product or service concentration.

- Provide prompt attention and remediation of risk behaviours by onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination of the agent.

- Provide guidelines and assistance to the agent to assess its own compliance program regime and to develop its own risk assessment based upon its unique risk profile for its products and services, customers, geography, and subagents or outlets (if applicable).

- Ensure compliance regime adherence to internal policies and external regulation, such as reporting suspicious or attempted suspicious activities, large transactions, monitoring the risk behaviours described above, reporting and recordkeeping, through periodic AML compliance program reviews.

130. The starting point is for a MSB to assess the risks that the agent may pose taking into consideration any appropriate risk variables before making a final determination. Assessing agent risk is more complex for those MSBs with an international presence due to varying jurisdictional requirements and the logistics of agent oversight. This agent risk analysis should include:

- A standard level of due diligence applied to all applicants, such as legal and ownership structure, soundness and AML/CFT compliance history.

- The standard level being reduced in recognized lower risk scenarios, such as conducting transactions for:

  - Publicly listed companies subject to regulatory disclosure requirements.
  - Other MSBs (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations and which are supervised for compliance with those requirements.

- An increased level of due diligence applied to those applicants determined to be higher risk, such as:
  - Agents located in a higher-risk jurisdiction.
  - Principals determined to have PEP status.
  - Agents with a history of regulatory noncompliance.
  - Agents serving high-risk customers or transactions as described in 110 to 112 above.

Agent Monitoring

131. Agent monitoring is a very important element in an effective MSB AML/CFT program. While all agents require baseline monitoring to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance, the risk-based approach requires a higher level of monitoring to locate and eliminate the few agents that knowingly or through willful blindness act in a way that may conceal their customers' conduct from routine monitoring. The degree and nature of agent monitoring will depend on the transaction volume and principal volume of the agent with whom the MSB shares responsibility for effective AML/CFT, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent, such as the products or services being provided by the agent, the location of the agent and the nature of the activity.

132. The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each MSB's analysis of its major risks. Regulatory authorities should, therefore, be mindful of and give due weight to the determinations made by MSBs, provided that these determinations are consistent with any legislative or regulatory requirements, and are reasonable and adequately documented.

133. Agent monitoring under a risk-based approach allows a MSB to create monetary or other thresholds to determine which agent activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MSBs should also assess the adequacy and integrity of any systems and processes on a periodic basis.

134. Agent monitoring under a risk-based approach should utilize baseline risk assessment tools that monitor agent activity to measure transaction-related risk or identify agents that exhibit risk behaviours, such as those described in para. 113 above, structured transactions, customer identification sharing or biographical information sharing, higher volume senders or payees, unusual and unexplained spikes in transaction volume, inferior data quality entered at point of origination, related STR/SAR activity, higher volume agent-to-agent corridors, unusual agent patterns, or unusual product or service concentration. Prompt attention and remediation of risk behaviours should be addressed by appropriate means, such as enhanced examination of the agent's transaction history and data integrity, to learn and evaluate the agent's explanation of these concerns, confidential sampling of the questioned aspects of the agent's services, or

onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination.

Training and Awareness

135. MSBs should provide agents appropriate training with regard to ML/TF. A MSB's commitment to having and maintaining successful controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees and agents with at least general information on AML/CFT laws, regulations and internal policies.

136. Applying a risk-based approach to the various methods available for training gives each MSB additional flexibility regarding the frequency, delivery mechanisms and focus of such training. Agent training should be documented and training records should be maintained according to applicable record keeping requirements. A MSB should review its agent base and available resources and implement training programmes that provide appropriate AML/CFT information that is at the appropriate level of detail.

137. Agent training may include onsite or offsite initial training (*i.e.* upon activation), and ongoing training via web-based programmes, periodic mailings or newsletters, password-protected informational websites or pop-up messages at point of origination. In conjunction with or in addition to such training, the MSB may provide periodic compliance program reviews involving a comprehensive assessment of the agent's compliance with internal and external AML regulatory requirements.

Chapter Three: Internal Controls

138. In order for MSB 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 MSB 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 MSB's policies, procedures and processes designed to limit and control risks.

139. 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 MSB's business.
- The diversity of a MSB's operations, including geographical diversity.
- The MSB's customer, product and activity profile.
- The distribution channels used.
- The volume and size of the transactions.
- The degree of risk associated with each area of the MSB's operation.
- The integrity of the systems used.
- The extent to which the MSB is dealing directly with the customer or is dealing through intermediaries, third parties, or in a non face-to-face setting.

140. The framework of internal controls should:

- Provide increased focus on a MSB's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers, terrorist financiers, and other criminals.
- Provide for regular review of the risk assessment and risk management processes, taking into account the environment within which the MSB operates and the activity in its market place.
- Designate an individual or individuals at management level responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme.
- Ensure that adequate controls are in place before new products are offered.
- Inform senior management of compliance initiatives, 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 all regulatory record keeping and reporting requirements and recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.

- Provide for adequate controls for higher risk customers, transactions and products, agents, 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 management and oversight of its agents, including initial Know Your agent due diligence, AML/CFT training, and ongoing risk-based monitoring.

- Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the business's AML/CFT programme.

- Develop and implement written AML/CFT policies, procedures and processes, with periodic internal testing to ensure adherence by all staff with AML/CFT-related responsibilities.

- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.

- Provide for appropriate initial and refresher training to be given to all relevant staff.

- Provide for appropriate initial and refresher training for agents at appropriate intervals.

141. 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 MSB. 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 MSB's AML/CFT compliance programme. The testing should be risk-based (focusing attention on higher-risk customers, geography, products and services, agents); should evaluate the adequacy of the MSB's overall AML/CFT programme; and the quality of risk management for the MSB's operations, departments and subsidiaries; include comprehensive procedures and testing; and cover all activities.

REFERENCES

FATF (2009), *AML/CFT Evaluations and Assessments - Handbook for Countries and Assessors*, FATF, Paris, **www.fatf-gafi.org/dataoecd/46/24/40978997.pdf**.

FATF (2009), *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*, FATF, Paris, **www.fatf-gafi.org/dataoecd/16/54/40339628.pdf**.

FATF, *40 Recommendations*, FATF, Paris,
www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

FATF, *9 Special Recommendations*, FATF, Paris
www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html

FATF, *40 Recommendations Glossary*, FATF, Paris,
www.fatf-gafi.org/glossary/0,3414,en_32250379_32236889_35433764_1_1_1_1,00.html.

FATF (2008), *Report on Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris, **www.fatf-gafi.org/dataoecd/46/24/40978997.pdf** .

ANNEX 1

SOURCES OF FURTHER INFORMATION

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

www.fatf-gafi.org

FATF typologie report on Alternative Remittances Systems (June 2005):
http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf

B. Legislation/Guidance on the Risk-Based Approach

Delegations are invited to indicate in this section possible website links to legislation / guidance that have been produced on Risk-Based Approach for the MSB sector or on Risk Assessment Analysis.

Australia: See *http://austrac.gov.au/courses.html*

Belgium: See *Money laundering indicators* issued by the Belgian FIU (***www.ctif-cfi.be/doc/en/typo_ctif_cfi/NL1175eENG.pdf***), and the circular of the Belgian Supervisory Authority (CBFA) on the obligations of customer due diligence and on preventing the use of the financial system for money-laundering and the financing of terrorism **(*www.cbfa.be/eng/wk/circ/wk_circ.asp*).**

Brazil: See ***www.bcb.gov.br/?RMCCIINORMS*** *(English) or* ***www.bcb.gov.br/rex/rmcci/port/rmcci.asp*** *(Portuguese)*

Canada: See *FINTRAC guidelines* **(***www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp#66***)**

Denmark: See *Indicators on possible money laundering or financing of terrorism* issued by the Danish FIU **(www.dfsa.dk/sw41296.asp**)

Norway: See *Guidelines to the new Money Laundering Act and Regulation, including guidelines on the risk-based approach:*
(www.kredittilsynet.no/Global/Venstremeny/Rundskriv%20-%20vedlegg/23062009_Rundskriv_8_2009_Endelig.pdf) (Norwegian only)

United Kingdom: See the Guidelines issued by HM Revenue and Customs at ***www.hmrc.gov.uk/mlr/mlr8.pdf***

United States: In December 2008, the Financial Crimes Enforcement Network (FinCEN) released a manual to provide guidance to officials examining money services businesses (MSBs) for compliance with the requirements of the Bank Secrecy Act (BSA). The following is a link to the Manual: **www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf**
General MSB information is also available via FinCEN's homepage; the website references all MSB guidance and additional MSB educational materials.
See **www.fincen.gov/financial_institutions/msb/**.

C. Other Sources of Information to help assist national and financial institution risk assessment of countries and cross border activities

In determining the levels of risks associated with particular country or cross border activity financial institutions 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: *www1.worldbank.org/finance/html/cntrynew2.html*,
  - International Monetary Fund: *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)
     www.apgml.org/documents/default.aspx?DocumentCategoryID=8
  2. Caribbean Financial Action Task Force (CFATF)
     www.cfatf.org/profiles/profiles.asp
  3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)
     www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/5_money_laundering/Evaluations/Reports_summaries3.asp#TopOfPage

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

5. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
   www.esaamlg.org/reports/me.php

6. GAFISUD
   www.gafisud.org/actividades.asp

7. Inter-governemental Actions Group against Money Laundering in West Africa (GIABA)
   www.giaba.org/index.php?type=c&id=24&mod=2&men=1

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

- OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting).

  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).

  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.

  www.egmontgroup.org/

- Signatory to the United Nations Convention against Transnational Organized Crime

  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

  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:

  www.un.org/sc/committees/

- Transparency International – the global civil society organisation leading the fight against corruption, brings people together in a powerful worldwide coalition to end the devastating impact of corruption on men, women and children around the world. TI's mission is to create change towards a world free of corruption.

  www.transparency.org/

ANNEX 2

GLOSSARY OF TERMINOLOGY

Agent

For the purposes of Special Recommendation VI, an agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licencees, franchisees, concessionaires). (This definition is drawn from the Interpretative Note to SR. VI. It is used in the criteria under SR VI).

Batch transfer

A batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.

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.

Core Principles

The Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organisation of Securities Commissions, and the Insurance Core Principles issued by the International Association of Insurance Supervisors.

Cross-border transfer

Cross-border transfers means any wire transfer where the originator and beneficiairy institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.

Currency

Currency refers to banknotes and coins that are in circulation as a medium of exchange.

Designated Threshold

The amount set out in the Interpretative Notes to the FATF Recommendations.

Domestic transfer

Domestic transfer means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction.

FATF Recommendations

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

Financial Institutions

Any person or an agent who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (*e.g.* credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   - Money market instruments (cheques, bills, CDs, derivatives etc.).
   - Foreign exchange.
   - Exchange, interest rate and index instruments.
   - Transferable securities.
   - Commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.

11. Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance.[9]

13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

Footnotes:

[5] This also captures private banking.

[6] *This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance* of commercial transactions (including forfaiting).

[7] This does not extend to financial leasing arrangements in relation to consumer products.

[8] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

[9] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Funds transfer

The terms *fund transfer* refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

Legal Arrangements

Legal arrangements refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include *fiducie, treuhand and fideicomiso*.

Legal Persons

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.

Originator

The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

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.

Supervisors/Regulators

The designated competent authorities who have responsibility for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

Unique identifier

For the purposes of Special Recommendation VII, a unique identifier refers to any unique combination of letters, numbers or symbols that refers to a specific originator.

Wire transfer

For the purpose of Special Recommendation VII, the terms wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

ANNEX 3

MEMBERSHIP OF THE ELECTRONIC ADVISORY GROUP

FATF Members & Observers

Argentina, Belgium, Canada, France, Portugal, Spain, UK, US, GIABA, MENAFATF, MONEYVAL, OGBS, UN, World Bank.

Money Services Business Sector

Canada	Money Services Round Table
	Cash Money
	Custom House Ltd.
	Independent Financial Brokers
	Travelex Worldwide Money
	The Western Union Company
Germany	GDV
South Africa	Asisa
	Moneygram
US	Financial Service Centers of America (FiSCA)
	Howrey LLP
	Moneygram
	National Money Transmitters Association, Inc
	Optima Compliance & Consulting, Inc.
	The Western Union Company