Financial Action Task Force

Groupe d'action financière

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

High Level Principles and Procedures

JUNE 2007

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

High Level Principles and Procedures

This Guidance was developed by the FATF in close consultation with representatives of the international banking and securities sectors. This public-private sector partnership was integrally involved in the development and finalisation of the Guidance. A list of members of that group is attached at Annex 5. The Guidance Paper was adopted by the FATF at its June 2007 Plenary.

TABLE OF CONTENTS

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

Chapter One: Background and Context

1.1 Following a meeting in December 2005 between the FATF and representatives of the banking and securities sectors, FATF agreed to establish an Electronic Advisory Group (EAG) on the risk-based approach as part of its outreach to the private sector. The EAG, which is a sub-group of the FATF Working Group on Evaluations and Implementation (WGEI) was set up in March 2006, and was chaired by Mr. Philip Robinson (Financial Services Authority, United Kingdom) and Mr. Rick Small (GE Money, United States). Membership of the Group has consisted of FATF members and observers, as well as representatives from the banking and securities sectors that volunteered to work on the issue of the risk-based approach to combating money laundering and terrorist financing (referred to throughout this paper as "the risk-based approach" (RBA)). A list of members is attached at Appendix 5.

1.2 The work of the EAG followed a number of steps: responses to a questionnaire on risk-based approach were obtained, then the high level elements of a risk-based approach were identified and an outline of the EAG report was agreed. There then followed extensive consultation with both public and private sector members of the EAG, and a final report of the EAG to WGEI setting out draft guidance on the implementation of a risk based approach was provided in April 2007. After further international consultation with both public and private sectors, this Guidance Paper was adopted by the FATF at its June 2007 Plenary. This is the first occasion that the FATF has developed guidance using a public-private sector partnership approach.

Purpose of the Guidance:

1.3 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. And
- Indicate good public and private sector practice in the design and implementation of an effective risk-based approach.

Target Audience, Status and Content of the Guidance:

1.4 The Guidance is primarily addressed to public authorities and financial institutions. However, many of the high level principles contained in this document will be equally applicable to designated non-financial businesses and professions. 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 which to interpret section two (Guidance for Public Authorities) and section three (Guidance for Financial Institutions). There is also Annex 1, which contains descriptions of additional sources of information.

1.5 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 financial institutions may wish to consider when applying a risk-based approach.

1.6 The Guidance recognises that each country and its national authorities, in partnership with its financial institutions, 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

1.7 The FATF Recommendations contain language that permits countries to some degree to adopt a risk-based approach to combating money laundering and terrorist financing. That language also authorise countries to permit financial institutions 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 financial institutions 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 financial institutions, 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.

1.8 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.

1.9 A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. Countries will need to identify the main vulnerabilities and address them accordingly. Institutions 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.

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

1.11 Proportionate procedures should be designed based on assessed risk. Higher risk areas should be subject to enhanced procedures: for the financial services sector, this would include measures such as enhanced customer due diligence checks and enhanced transaction monitoring. It also follows that in instances where risks are low, simplified or reduced controls may be applied.

1.12 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 financial institutions 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 financial institutions with regard to managing potential money laundering and terrorist financing risks and allow financial institutions to exercise reasonable business judgement with respect to their customers. A risk-based approach should not be designed to prohibit financial institutions

from engaging in transactions with customers or establishing relationships with potential customers, but rather it should assist financial institutions to effectively manage potential money laundering and terrorist financing risks.

1.13 Regardless of the strength and effectiveness of AML/CFT controls established by financial institutions, 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 financial institution's well-reasoned risk-based approach. When financial institutions 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:

1.14 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 financial institutions 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.

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

1.16 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 financial institutions. Without cooperation and understanding between these parties, there can be no effective risk-based process.

1.17 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 financial institutions 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 financial institutions to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

Challenges:

1.18 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 1.34 to 1.38 below.

1.19 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 open or maintain an account.

1.20 Implementing a risk-based approach requires that financial institutions have a good understanding of the risks and are able to exercise sound judgment. This requires the building of expertise within financial institutions, 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 financial institutions making flawed judgments. Firms may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, thereby creating vulnerabilities.

1.21 Financial institutions 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 financial institution that allows for inadequate resources to be devoted to compliance leading to potentially significant compliance failures. Supervisors should place greater emphasis on whether the financial institution has an effective decision-making process. However, sample testing should be used or individual decisions reviewed as a means to test the effectiveness of the institution’s overall risk management (see paragraph 2.47). Supervisors should appreciate that even though the financial institution has established appropriate risk management structures and procedures that are regularly updated, and has followed the relevant policies, procedures, and processes, the financial institution may still make decisions that were incorrect in light of additional information not reasonably available at the time.

1.22 In implementing the risk-based approach financial institutions should be given the opportunity to make reasonable judgments. This will mean that no two financial institutions 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 financial institution 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.
- Financial institution focus on real and identified threats.
- Flexibility to adapt to risks that change over time.

Potential Challenges:

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

Chapter Three: FATF and the Risk-Based Approach

1.23 The varying degrees of risk of money laundering or terrorist financing for particular types of financial institutions 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 financial institutions (only), 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).

General Risk Principle

1.24 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

1.25 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

[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).

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 financial institutions (R.12, 16 & 24).

Customer Due Diligence (R.5-9)

1.26 Risk is referred to in several forms:

a. Higher risk – Under Recommendation 5, a country must require its financial institutions to perform enhanced due diligence for higher-risk customers, business relationships or transactions. Recommendations 6 (Political exposed persons) and 7 (Correspondent banking) are examples of this principle and are considered to be higher risk scenarios requiring enhanced CDD.

b. Lower risk – a country may also permit its financial institutions to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). Financial institutions 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 financial institutions 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 financial institutions 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 financial institutions to determine the degree of risk and how they manage that risk, as well as to review the determinations made by institutions. This expectation applies to all areas where the risk-based approach applies. In addition, where the competent authorities have issued guidelines to financial institutions on a suitable approach to risk-based procedures, it will be important to establish that the financial institutions have indeed followed such guidelines. The Recommendations also recognise that country risk is a necessary component of any risk assessment mechanism (R.5 & 9).

Institutions' internal control systems (R.15 & 22)

1.27 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 institutions to have regards 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)

1.28 Under Recommendation 23 (for financial institutions other than those subject to the Core Principles or persons providing money or value transfer services), 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 institutions 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.

1.29 Recommendation 23 also recognises that financial institutions subject to Core Principles should also apply elements of the Core Principles that are relevant to AML/CFT (and which are not expressly covered by the FATF Recommendations) for the purpose of combating money laundering and terrorist financing *e.g.* licensing of institutions. Moreover, the Core Principles set out sound principles relating to the procedures for assessing and managing risk, and consideration could be given as to how those already well-defined concepts could apply to AML/CFT.

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

1.30 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]

1.31 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

1.32 As regards the FATF Nine Special Recommendations on Terrorist Financing, 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.

1.33 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

3 Handbook paragraph 42(e) (i).

4 See Methodology R.24.

5 Handbook paragraph 42 (f).

will be filed. As well as being an essential input to any assessment of country or sector wide risks, the promptness and content of such feedback is relevant to implementing an effective risk-based approach.

Applicability of the risk-based approach to terrorist financing

1.34 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.

1.35 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 financial institution to determine the type of underlying criminal activity, or intended terrorist purpose, rather the institution'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.

1.36 Therefore, the ability of financial institutions 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).

1.37 Where particular individuals, organisations or countries are the subject of terrorist finance sanctions, the obligations on institutions 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.

1.38 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. Financial institutions 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

1.39 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.

1.40 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.

1.41 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. 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.

1.42 Countries may allow financial institutions 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 account purpose, 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.

1.43 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 financial institution. 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

1.44 Risk-based policies and processes in financial institutions should be distinguished from risk-based supervision. As illustrated through the 2006 revision of the Basel Core Principles there is a general recognition within supervisory practice of allocating resources taking into account the risks posed by individual financial institutions.[6] 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 financial institutions. 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 financial institutions are exposed. Consequently, this prioritisation would lead supervisors to demonstrate increased regulatory attention to financial institutions that engage in activities assessed to be of higher money laundering risks.

1.45 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.

1.46 Since prudential regulators should have already assessed the quality of risk management controls throughout the financial institutions, it is reasonable that their assessments of these controls be used, at least in part, to inform money laundering and terrorist financing risk assessments (see also paragraph 1.26 above). *Annex 2, provides an example of an assessment that regulators may wish to consider when prioritising supervisory work.*

Summary box:

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

- Financial institutions 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 financial institutions 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 financial institutions.
- Requirements and supervisory oversight at the national level should be consistent among similar industries.

[6] See for example *Core Principles Methodology* 2006, Principle 1(1), footnote 6 to AC.

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

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

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

2.2 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. For example, discussion in this paper assumes that the financial services industry is part of the private sector, although in many countries at least some financial institutions are state-owned.

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

2.3 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.

2.4 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.

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

2.5 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 financial institutions should be informed by the outcomes of the national risk assessment.

2.6 The risk-based approach does not mean the absence of a clear statement of what is required from financial institutions. However under a risk-based approach, financial institutions 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 particular financial institution/business. 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.

2.7 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

2.8 Where competent authorities have been assigned responsibility for overseeing financial institutions' 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.

2.9 Where appropriate, regulators should seek to adopt a risk-based approach to the supervision of financial institutions' controls to combat money laundering and terrorist financing. This should be based on a thorough and comprehensive understanding of the types of financial activity, the financial and other institutions that undertake such activity and the money laundering and terrorist financing risks to which these are exposed. 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.

2.10 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.

2.11 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.

2.12 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 financial institution that has adopted a risk-based approach. These decisions will cover the adequacy of financial institutions' 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 a financial institution.

Principle Four: Identifying the main actors and ensuring consistency

2.13 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 may be shared to best effect. For example, which body or bodies are best placed to provide guidance to the financial services industry about

[7] See FATF Recommendation 30.

how to implement a risk-based approach to anti money laundering and counter- terrorist financing.

2.14 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 private sector – this might include financial services firms, professional services firms (such as accountants and lawyers), trade bodies, etc.
- The public – arrangements designed to counter money laundering and terrorist financing are ultimately designed to protect the law-abiding public. However these arrangements may also act to place burdens on customers of financial services 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.

2.15 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.

2.16 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:

- Financial institutions 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 financial institution'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 financial institution with good controls aimed at preventing money laundering and the finance of terrorism is able to achieve. A financial institution 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

2.17 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.

2.18 Public authorities, whether law enforcement agencies, regulators or other bodies, have privileged access to information that may assist financial institutions to reach informed

judgments when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, financial institutions routinely transact with a great number of customers on a daily basis, and are able to understand their clients' businesses reasonably well. It is desirable that public and private bodies work collaboratively to identify what information is valuable to help combat money laundering and terrorist financing, and to develop means by which this information might be shared in a timely and effective manner.

2.19 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.

2.20 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 financial institutions.
- Countries, persons or organisations whose assets or transactions should be frozen.

2.21 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 financial institutions' decision making processes, along with any other relevant information that is available to the financial institutions.

Chapter Two: Implementation of the Risk-Based Approach

Assessment of Risk to Inform National Priorities:

2.22 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 financial institutions. 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'.

2.23 A national risk assessment should be regarded as a description of fundamental background information to assist supervisors, law enforcement authorities, the FIU and financial institutions to ensure that decisions about allocating responsibilities and resources at the

[8] Examples of such dialogue are included in section four of these guidelines.

national level are based on a practical, comprehensive and up-to-date understanding of the risks.

2.24 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 financial institutions.
- Corporate governance arrangements in financial institutions 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.

2.25 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.

2.26 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.

2.27 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, regulators and financial institutions, 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.

2.28 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.

2.29 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

2.30 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.

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

2.32 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.

2.33 Competent authorities expect financial institutions 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 financial institutions 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.

2.34 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 financial institutions 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 open an account in a different country).
- Politically exposed persons (to apply a specific policy); And
- 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

2.35 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.

2.36 In the course of their examinations, supervisors should review a financial institution'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 financial institution and the adequacy of its mitigation measures. Where available, assessments carried out by or for the institutions may be a useful source of information. The assessment should include sample transaction testing of customer accounts 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.

2.37 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.

2.38 Supervisors should be in a position to compare risk factors and procedures used by peer financial institutions. This will, among other objectives, assist the supervisors in better understanding how financial institutions 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 financial institution's money laundering and terrorist financing risk assessment, with the understanding, however, that they may possess information that has not been made available to financial institutions and, therefore, financial institutions 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

[9] See Basel Core Principle 20 on Supervisory techniques.

encouraged to use that knowledge to issue guidelines to assist financial institutions in managing their risks. Where financial institutions 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 institutions 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.

2.39 In the context of the risk-based approach, the primary focus for supervisors should be to determine whether or not the financial institution'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 financial institutions have adequately and effectively implemented appropriate risk mitigation strategies.

2.40 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 supervisory tools for use when, in the supervisor's judgement, a bank is not complying with laws, regulations or supervisory decision […]. These tools include the ability to require a bank 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".[11]

2.41 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.

2.42 A number of generic aspects of proportionate supervisory actions have been set out in the Basel Core Principles Methodology (as revised October 2006). Although not directly related to anti-money laundering, they nonetheless offer helpful insights into the supervisory oversight of associated risk management process. The key concepts drawn from these principles are outlined in Appendix One.

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

a) Regulatory Transparency

2.44 In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Supervisors are aware that financial institutions, 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.

2.45 No matter what individual procedure is adopted, the guiding principle will be that financial institutions 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

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

[11] Basel *Core Principles Methodology* 2006, Principle 23, EC 3.

disproportionate or unpredictable which may undermine even the most effective application of the risk-based approach by financial institutions.

b) Staff Training of Supervisors and Enforcement Staff

2.46 In the context of the risk-based approach, it is not possible to specify precisely what a financial institution 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.

2.47 Training should aim to allow supervisory staff to form sound comparative judgements about financial institutions 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 institutions 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 institutions' arrangements.

2.48 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".[12] 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 bank or banking group to strengthen them".[13] Supervisors also should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

2.49 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 financial institution'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.

[12] See R.29 and *Customer due diligence for banks*, § 61.

[13] Basel Core Principle Methodology, Core Principle 7, EC1.

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, and correspondent banking
- 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 financial institution is meeting any minimum regulatory requirements (b) the financial institution 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.

Appendix One: Key aspects of risk management as described in the Basel Core *Principles Methodology* (as revised in October 2006):

Excerpts on risk management processes:

"Individual banks and banking groups are required to have in place comprehensive risk management policies and processes to identify, evaluate, monitor and control or mitigate material risks. The supervisor determines that these processes are adequate for the size and nature of the activities of the bank and banking group and are periodically adjusted in the light of the changing risk profile of the bank or banking group and external market developments. If the supervisor determines that the risk management processes are inadequate, it has the power to require a bank or banking group to strengthen them." (Principle 7, Essential Criteria 1).

"The supervisor confirms that banks and banking groups have appropriate risk management strategies that have been approved by the Board. The supervisor also confirms that the Board ensures that policies and processes for risk-taking are developed, appropriate limits are established, and senior management takes the steps necessary to monitor and control all material risks consistent with the approved strategies." (CP7, EC2);

"The supervisor determines that risk management strategies, policies, processes and limits are properly documented, reviewed and updated, communicated within the bank and banking group, and adhered to in practice. The supervisor determines that exceptions to established policies, processes and limits receive the prompt attention of and authorisation by the appropriate level of management and the Board where necessary." (CP7, EC3).

"The supervisor determines that senior management and the Board understand the nature and level of risk being taken by the bank […]. The supervisor also determines that senior management ensures that the risk management policies and processes are appropriate in the light of the bank's risk profile and business plan and that they are implemented effectively. This includes a requirement that senior management regularly reviews and understands the implications (and limitations) of the risk management information that it receives. The same requirement applies to the Board in relation to risk management information presented to it in a format suitable for Board oversight." (CP7, EC4).

"Where banks and banking groups use models to measure components of risk, the supervisor determines that banks perform periodic and independent validation and testing of the models and systems." (CP7, EC6).

"The supervisor determines that banks and banking groups have risk evaluation, monitoring, and control or mitigation functions with duties clearly segregated from risk-taking functions in the bank […]" (CP7, EC9).

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

Preamble

3.1 The specifics of a financial institution's particular risk-based process should be determined based on the operations of the financial institution. Where appropriate and feasible, these policies, procedures and controls setting out how an institution will manage and mitigate its money laundering and terrorist financing risks should be articulated on a 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 1.34 through 1.38). A reasonably designed risk-based approach provides the means by which a financial institution identifies the criteria to assess potential money laundering risks. A reasonably implemented risk-based process also provides a framework for identifying the degree of potential money laundering risks associated with customers and transactions and allows for an institution to focus on those customers and transactions that potentially pose the greatest risk of money laundering.

Chapter One: Risk Categories

3.2 In order to implement a reasonable risk-based approach, financial institutions should identify the criteria to assess potential money laundering risks. Identification of the money laundering and terrorist financing risks, to the extent that such terrorist financing risk can be identified, of customers or categories of customers, and transactions will allow financial institutions to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making monitoring of customer transactions and on-going reviews a fundamental component of a reasonably designed risk-based approach. A financial institution may also have to adjust its risk assessment of a particular customer based upon information received from a competent authority.

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

3.4 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

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

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN"). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by a financial institution because of the standing of the issuer and the nature of the measures.
- Countries identified by credible sources[14] as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

Customer Risk

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

- Customers conducting their business relationship or transactions in unusual circumstances, such as:
  - Significant and unexplained geographic distance between the institution and the location of the customer.
  - Frequent and unexplained movement of accounts to different institutions. And
  - Frequent and unexplained movement of funds between institutions in various geographic locations.

- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.

- Cash (and cash equivalent) intensive businesses including:

[14] "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 regulation and should not be viewed as an automatic determination that something is of higher risk.

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

- Charities and other "not for profit" organisations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis)[15].

- "Gatekeepers" such as accountants, lawyers, or other professionals holding accounts at a financial institution, acting on behalf of their clients, and where the financial institution places unreasonable reliance on the gatekeeper.

- Use of intermediaries within the relationship who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised.

- Customers that are Politically Exposed Persons (PEPs).

Product/Service Risk

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

- Services identified by competent authorities or other credible sources as being potentially higher risk, including, for example:
  - International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank) and pouch activities. And
  - International private banking services.

- Services involving banknote and precious metal trading and delivery.

- Services that inherently have provided more anonymity or can readily cross international borders, such as online banking, stored value cards, international wire transfers, private investment companies and trusts.

Variables That May Impact Risk

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

[15] See Special Recommendation VIII.

- The purpose of an account or relationship may influence the assessed risk. Accounts opened primarily to facilitate traditional, low denominated consumer transactions may pose a lower risk than an account opened to facilitate large cash transactions from a previously unknown commercial entity.

- The level of assets to be deposited by a particular customer or the size of transactions undertaken. Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow for a financial institution to treat the customer as lower risk.

- The level of regulation or other oversight or governance regime to which a customer is subject. A customer that is a financial institution regulated in a country with a satisfactory AML regime poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation. Additionally, companies and their wholly owned subsidiaries that are publicly owned and traded on a recognized exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate, recognised regulatory scheme, and, therefore, generally pose less risk due to the type of business they conduct and the wider governance regime to which they are subject. Similarly, these entities may not be subject to as stringent account opening due diligence or transaction monitoring during the course of the relationship.

- The regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering perspective.

- The familiarity with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a financial institution's own operations within the country.

- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

Controls for Higher Risk Situations

3.9 Financial institutions should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as the result of the institution's risk-based approach. These measures and controls may include:

- Increased awareness by the financial institution of higher risk customers and transactions within business lines across the institution.
- Increased levels of know your customer (KYC) or enhanced due diligence.
- Escalation for approval of the establishment of an account or relationship.
- Increased monitoring of transactions.
- Increased levels of ongoing controls and frequency of reviews of relationships.

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

Chapter Two: Application of a Risk-Based Approach

Customer Due Diligence/Know Your Customer

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

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

(b) Take reasonable risk based measures to identify and verify the identity of any beneficial owner. And

(c) Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions.

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

- A standard level of due diligence, to be applied to all customers.
- The standard level being reduced in recognized lower risk scenarios, such as:
  - 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.
  - Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds.
  - Transactions involving de minimis amounts for particular types of transactions (*e.g.* small insurance premiums).
- An increased level of due diligence in respect of those customers that are determined to be of higher risk. This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as:
  - Correspondent banking relationships; and
  - PEPs.

Monitoring of Customers and Transactions

3.12 The degree and nature of monitoring by a financial institution will depend on the size of the financial institution, the AML/CFT risks that the institution 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, financial institutions 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 and the location of the customer and the transactions. Monitoring methodologies and processes also need to take into account the resources of the financial institution.

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

3.14 Monitoring under a risk-based approach allows a financial institution to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine adequacy for the risk levels established. Financial institutions should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented.

Suspicious Transaction Reporting

3.15 The reporting of suspicious transactions or activity is critical to a country's ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. Countries' reporting regimes are laid down in national law, requiring institutions to file reports when the threshold of suspicion is reached.

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

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

Training and Awareness

3.18 Recommendation 15 requires that financial institutions provide their employees with AML/CFT training, and it is important that financial institution employees receive appropriate and proportional training with regard to money laundering and terrorist financing. A financial institution's commitment to having successful controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees with at least general information on AML/CFT laws, regulations and internal policies.

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

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

Chapter Three: Internal Controls

3.20 In order for financial institutions 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 financial institution 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 financial institution's policies, procedures and processes designed to limit and control risks.

3.21 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 financial institution's business.
- The diversity of a financial institution’s operations, including geographical diversity.
- The financial institution’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 financial institution’s operation.
- The extent to which the financial institution is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non face to face access.

3.22 The framework of internal controls should:

- Provide increased focus on a financial institution's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
- Provide for regular review of the risk assessment and management processes, taking into account the environment within which the financial institution 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, recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence policies, procedures and processes.
- Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enable the timely identification of reportable transactions and ensure accurate filing of required reports.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the institution's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Provide for appropriate training to be given to all relevant staff.
- For groups, to the extent possible, there should be a common control framework.

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

ANNEXES

Annex 1

Sources of Further Information

4.1 Various sources of information exist that may help both countries and financial institutions 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 financial institutions 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.

http://www.fatf-gafi.org

B. International Bodies/Organisations

Basel Committee

The Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide. It seeks to do so by exchanging information on national supervisory issues, approaches and techniques, with a view to promoting common understanding. At times, the Committee uses this common understanding to develop guidelines and supervisory standards in areas where they are considered desirable. In this regard, the Committee is best known for its international standards on capital adequacy (Basel I and Basel II); the Core Principles for Effective Banking Supervision; the Concordat on cross-border banking supervision and other relevant documents related to risk management and AML/CFT.

http://www.bis.org/bcbs/

IOSCO

The International Organisation of Securities Commissions consists of capital market regulators, their aim is to promote high standards of regulation in order to maintain just, efficient and sound markets; to exchange information on their respective experiences in order to promote the development of domestic markets; to unite their efforts to establish standards and an effective surveillance of international securities transactions; and to provide mutual assistance to promote the integrity of the markets by a rigorous application of the standards and by effective enforcement against offences. IOSCO is known for Resolution on money laundering (1992) and AML Guidance for collective investment schemes (2005) which also address low-risk situations.

http://www.iosco.org/

IAIS

International Association of Insurance Supervisors represents some 180 insurance regulators and supervisors of more than 130 countries. Its objectives are to cooperate and contribute to improved supervision of the insurance industry on a domestic and international level in order to maintain efficient, fair, safe and stable insurance markets for the benefit and protection of policyholders; to promote the development of well-regarded insurance markets; and to contribute to global financial stability. IAIS has published principles (*e.g.* Insurance Core Principles and Methodology), standards (*e.g.* Supervisory standard on fit and proper requirements and assessment for insurers) and guidance papers (*e.g.* Guidance paper on AML/CFT; Guidance paper on combating the misuse of insurers; Guidance paper on preventing, detecting and remedying fraud in insurance).

http://www.iaisweb.org/

Transparency International

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.

http://www.transparency.org/

C.Legislation/Guidance on the Risk-Based Approach

Australia

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (administered by the Australian Government Attorney-General's Department):
http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200627290?OpenDocument

The Anti-Money Laundering and Counter-Terrorism Financing Rules (administered by the Australian Transaction Reports and Analysis Centre):
http://www.austrac.gov.au/aml_ctf_rules.html

Belgium

Belgium circular of the Banking, Finance and Insurance Commission on the obligations of Customer Due Diligence and Preventing the use of the financial systems for money laundering and the financing of terrorism:
http://www.cbfa.be/eng/bo/circ/pdf/ppb_2004_8_d_250.pdf

Belgium regulation of the Banking, Finance and Insurance Commission Preventing money laundering and the financing of terrorism:
http://www.cbfa.be/eng/vt/vz/circ/pdf/regulations_27-07-2004.pdf

Canada

Canada, Office of the Superintendent of Financial Institutions – Guidelines on Deterring and Detecting Money Laundering and Terrorist Financing: Sound Business and Financial Practices
http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/B8_e.pdf

Germany

Federal Financial Supervisory Authority of Germany – BaFin. Internal implementation of appropriate risk management systems for the prevention of money laundering, the financing of terrorism and fraud at the expense of institutions pursuant to sec. 25a (1), sentence 3, No. 6, and (1a) of the Banking Act and sec. 14 (2), No. 2, of the Money Laundering Act
http://www.bafin.de/rundschreiben/89_2005/050324_en.htm

Anti-money laundering safeguards at credit institutions acting as correspondent banks
http://www.bafin.de/verlautbarungen/gw_001106_en.htm

Italy

Parts One and Two of the Bank of Italy's Guidance on Suspicious Activity Reports for all financial intermediaries operating in Italy.
http://www.bancaditalia.it/vigilanza_tutela/vig_ban/norma/provv;internal&action=lastLevel.action&Parameter=vigilanza_tutela

Japan

Japanese Financial Services Agency – legislation and guidance
http://www.fsa.go.jp/en/refer/legislation/index.html

Jersey

Financial Services Commission – Guidance note on anti money laundering:
http://www.jerseyfsc.org/the_commission/anti-money_laundering/guidance_notes/index.asp

South Africa

FIU – General Guidance Note Concerning the Identification of Clients
http://www.fic.gov.za/info/Guidance%20concerning%20identification%20of%20clients.pdf

Singapore

Singapore notice to banks on the prevention of money laundering and counter terrorist financing
http://www.mas.gov.sg/resource/legislation_guidelines/aml/626%20_amdd%20280207.pdf

Switzerland

Ordinance of the Swiss Federal Banking Commission Concerning the Prevention of Anti- Money Laundering:

http://www.ebk.admin.ch/e/archiv/2003/pdf/m032703-03e.pdf

United Kingdom, Joint Money Laundering Steering Group (JMLSG) Guidance

UK Industry guidance on anti-money laundering and counter terrorist financing covering good practice application of the law, regulatory requirements and anti-money laundering controls, considered an integral element of the UK AML risk-based approach framework.
http://www.jmlsg.org.uk

United States

FFIEC Bank Secrecy Act Anti-Money Laundering Examination Manual
http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf

Wolfsberg Group

The Wolfsberg Group is an association of 12 global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. In 2006 the Wolfsberg Group produced guidance on a risk-based approach for managing money laundering risks.
http://www.wolfsberg-principles.com/index.html

D.Information sharing/outreach arrangements between the public and private sector

Section 314 of the USA PATRIOT Act of 2001: Regulations implemented pursuant to section 314 established procedures for information sharing to deter money laundering and terrorist activity. These regulations increase information sharing in two respects: *i)* establishes a mechanism by which federal law enforcement agencies can solicit from financial institutions information related to suspected terrorist activity or money laundering; and, *ii)* encourages financial institutions to share information among themselves in order to identify and report activities that may involve terrorism or money laundering.
http://www.fincen.gov/po1044.htm

The United States Bank Secrecy Act Advisory Group: Established by the U.S. Congress in 1992, the Advisory Group is chaired by the Director of FinCEN (the US FIU) and serves as the principal forum in which issues related to the administration of the Bank Secrecy Act (BSA) are discussed amongst industry, regulators and law enforcement agencies. The Advisory Group provides advice to the Secretary of the Treasury on ways to enhance the utility of BSA data to law enforcement agencies while minimizing the impact of compliance obligations on affected financial institutions.
http://uscode.house.gov/download/pls/31C53.txt

Private Sector Dialogue Programmes: The U.S. has initiated AML/CFT dialogues linking U.S. regulators and financial institutions with their counterparts from the Middle East/North Africa (MENA) and Latin America. This series of outreach events aims to raise awareness of domestic and regional money laundering and terrorist financing risks, international AML/CFT standards and regional developments, and U.S. government policies and private sector measures to combat terrorist financing and money laundering:
http://www.treas.gov/press/releases/js4346.htm
http://www.usmenapsd.org/index2.html

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

4.2 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: **http://www1.worldbank.org/finance/html/cntrynew2.html**,
  - International Monetary Fund: **http://www.imf.org/external/np/rosc/rosc.asp?sort=topic#RR**
  - Offshore Financial Centres (OFCs) IMF staff assessments **www.imf.org/external/np/ofca/ofca.asp**.

- Mutual evaluation reports issued by FATF Style Regional Bodies:

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

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

  3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)
  http://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)
  http://www.eurasiangroup.org/index-7.htm

  5. GAFISUD
  http://www.gafisud.org/miembros.htm

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

- OECD Sub Group of Country Risk Classification (a list of country of risk classifications published after each meeting)
  http://www.oecd.org/document/49/0,2340,en_2649_34171_1901105_1_1_1_1,00.html

- International Narcotics Control Strategy Report (published annually by the US State Department)
  http://www.state.gov/p/inl/rls/nrcrpt/

- Egmont Group membership - Coalition of FIU's that participate in regular information exchange and the sharing of good practice, acceptance as a member of the Egmont Group is based a formal procedure that countries must go through in order to be acknowledged as meeting the Egmont definition of an FIU.
  http://www.egmontgroup.org/

- Signatory to the United Nations Convention against Transnational Organized Crime
  http://www.unodc.org/unodc/crime_cicp_signatures_convention.html

- The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury economic and trade, Sanctions Programmes
  http://www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml

- Consolidated list of persons, groups and entities subject to EU Financial Sanctions
  http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm

- UN Security Council Sanctions Committee - Country Status:
  http://www.un.org/sc/committees/

Annex 2

Basel Committee on Banking Supervision – Working Group on Cross Border Banking - Risk Matrix

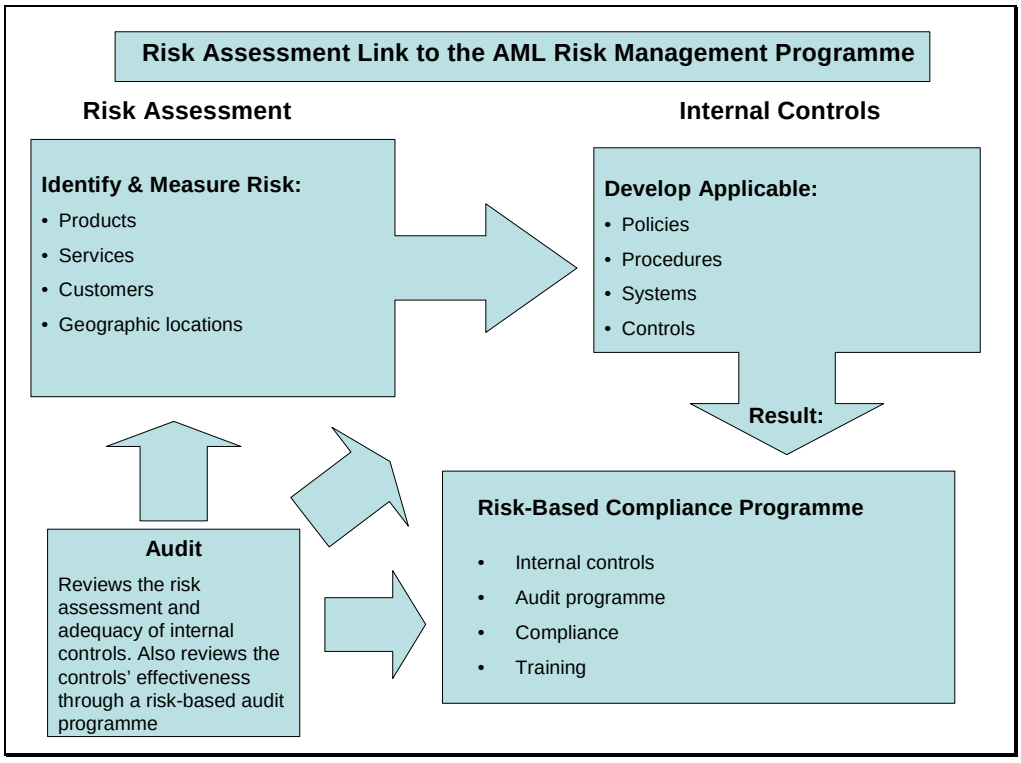
Analysis of specific risk categories that financial institutions and supervisory authorities may use in assessing AML risks:

Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the web site is informational or non-transactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment, or accounts opened via the Internet).
There are a few high-risk customers and businesses.	There are a moderate number of high-risk customers and businesses. These may include check cashers, convenience stores, money transmitters, casas de cambio, import or export companies, offshore corporations, politically exposed persons (PEPs), and foreign individuals.	There are a large number of high-risk customers and businesses. These may include check cashers, convenience stores, money transmitters, casas de cambio, import or export companies, offshore corporations, PEPs and foreign individuals.
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special-use accounts, or offer payable through accounts (PTAs).	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from low-risk countries, and minimal pouch activities, special-use accounts, or PTAs.	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML policies and procedures, particularly those located in high-risk countries, or offers substantial pouch activities, special-use accounts, or PTAs.
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank has full investment discretion.

Low	Moderate	High
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, non customers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of non-customer funds transfer transactions and payable upon proper identification (PUPID) transactions. Frequent funds from personal or business accounts to or from high-risk countries, and financial secrecy havens or countries.
No transactions with high-risk geographic locations.	Minimal transactions with high-risk geographic locations.	Significant volume of transactions with high-risk geographic locations.
Low turnover of key personnel or frontline personnel (i.e., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

Annex 3

Basel Committee on Banking Supervision – Working Group on Cross Border Banking - Risk Assessment Links to the AML Management Programme



Annex 4

Glossary of Terminology:

Beneficial Owner

The natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement

Competent authorities

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

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.

Designated Non-Financial Businesses and Professions

a. Casinos (which also includes internet casinos).
b. Real estate agents.
c. Dealers in precious metals.
d. Dealers in precious stones.
e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

Designated Threshold

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

FATF Recommendations

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

Financial Institutions

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

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
 - 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).

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.

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.

Shell Bank

Bank incorporated in a jurisdiction/country in which it has no physical presence and which is unaffiliated with a regulated financial group.

Supervisors/Regulators

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

Annex 5

Membership of the Electronic Advisory Group

FATF Members & Observers

Australia, Austria , Canada , European Commission, France, Germany, Italy, Japan, Mexico, Netherlands, South Africa, Sweden, Switzerland, UK, USA, IMF, IOSCO, OGBS, World Bank, BCBS

Banking industry

BNP Paribas, Banking Association of South Africa, Banks Association of Turkey, Fortis Ban, German Banking Association, Banque et Caisse d'Epargne de l'Etat (Luxembourg), WestLB AG, Crédit Agricole, Felaban/ Mexican Banking Association, Bank of America, Macquarie Bank, CIBC, Japanese Bankers Association, UBS, HSBC, IBFed, European Association of Co-operative Banks, Association of Banks in Singapore, European Association of Public Banks, Wolfsberg Group, European Banking Federation.

Securities industry

Investment Dealers Association of Canada, Australian Financial Markets Association, UBS, London Investment Banking Association, JPMorgan Chase & Co., Securities Industry Association, NYSE, ICSA.