Financial Action Task Force

Groupe d'action financière

RBA GUIDANCE FOR DEALERS IN PRECIOUS METAL AND STONES

17 June 2008

TABLE OF CONTENTS

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

HIGH LEVEL PRINCIPLES AND PROCEDURES FOR DEALERS IN PRECIOUS METALS AND DEALERS IN PRECIOUS STONES

SECTION ONE: USING THE GUIDANCE

PURPOSE OF THE RISK-BASED APPROACH

Chapter One: Background and Context

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

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

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

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

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

Purpose of the guidance

6. The purpose of this Guidance is to:

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

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

Target audience, status and content of the guidance

8. This Guidance is written at a high level to recognize the differing practices of dealers in precious metals and dealers in precious stones (hereinafter referred to as “dealers”) in different countries, and the different levels and forms of monitoring that may apply. Each country and its national authorities should aim to establish a partnership with its dealers that will be mutually beneficial to combating money laundering and terrorist financing.

9. The primary target audience of this guidance is dealers in precious metals and dealers in precious stones themselves, when they conduct activities which fall within the ambit of the FATF Recommendations, as described below. For purposes of this guidance, the term "dealer" encompasses a wide range of persons engaged in these businesses, from those who produce precious metals or precious stones at mining operations, to intermediate buyers and brokers, to precious stone cutters and polishers and precious metal refiners, to jewellery manufacturers who use precious metals and precious stones, to retail sellers to the public, to buyers and sellers in the secondary and scrap markets.

10. Recommendation 12 mandates that the requirements for customer due diligence, record-keeping, and paying attention to all complex, unusual large transactions set out in Recommendation 5, 6, and 8 to 11 apply to dealers in precious metals and dealers in precious stones when they engage in any cash transaction with a customer equal to or above USD/EUR 15 000.

11. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions (see paragraph 132) and internal AML/CFT controls, and Recommendation 21 regarding measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, apply to dealers in precious metals and dealers in precious stones when they engage in any cash transaction with a customer equal to or above the applicable designated threshold (USD/EUR 15 000).

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

Observation on the particular activities carried out by dealers

13. The following general observation about the different businesses carried out by dealers should help inform the approach. Consideration should also be given to the particular activities performed by dealers on a national basis.

14. Diamonds, jewels and precious metals have unique physical and commercial properties which carry value in small, easily transportable quantities. The worldwide trade varies from modern international transactions conducted through the financial system, to localized informal markets. Dealers range from very poor individuals in some of the most remote and troubled places on the planet, to the wealthiest individuals, to large multinational companies working in major financial centres. Transaction methods also range from anonymous exchanges of handfuls of stones or nuggets for cash, to exchange-based government-regulated deals.

15. A risk assessment is familiar to dealers in diamonds, jewels and precious metals because of the risks of theft and fraud. Risks of money laundering and terrorist financing should be added to those traditional industry concerns, in a more formal structured program. Diamond dealers in particular will be familiar with such a program in the worldwide Kimberley Process[1] which is designed to ameliorate risks of conflict finance in rough diamonds.

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

The purpose of the risk-based approach

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

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

18. A number of the DNFBP sectors are subject to regulatory or professional requirements which complement AML/CFT measures, e.g. in some countries dealers will be licensed and some of their activities will be overseen by government agencies. Where possible, it will be beneficial for dealers to devise their AML/CFT policies and procedures in a way that harmonises with other regulatory or professional requirements. A risk-based AML/CFT regime should help ensure that honest customers and counterparties can access the services provided by dealers, but creates barriers to those who seek to misuse these services.

19. 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. Dealers will need this assistance to help them to identify higher risk customers and

[1] A worldwide regulatory scheme that governs the movement of rough diamonds across international borders, adding a certificate of the legitimacy of the trade of the diamonds and a statement of value to all rough diamonds traded across borders. It is supplemented by dealer warranties applicable to polished diamonds and jewelry containing diamonds covering each trade down to retail sales. The Kimberley Process includes all significant dealers and countries involved in diamond mining, trading and processing, and its tracking and valuation system.

counterparties, 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.

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

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

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

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

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

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

<u>Potential benefits and challenges of the risk-based approach</u>

Benefits:

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

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

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

Challenges:

29. 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 42 to 46 below.

30. 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 of procedures and systems. It will certainly lead to a greater diversity in practice which should lead to innovations and improved compliance. However, it may also cause uncertainty regarding expectations, difficulty in applying uniform regulatory treatment, and a lack of understanding by customers and counterparties regarding information required.

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

32. Dealers 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.

33. However, in situations where management fails to recognise or underestimates the risks, a culture may develop that allows for inadequate resources to be devoted to compliance, leading to potentially significant compliance failures.

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

35. In implementing the risk-based approach, dealers should be given the opportunity to make reasonable judgments with respect to their particular situations. This may mean that no two dealers in precious metals or dealers in precious stones or no two businesses within the same sector are likely to

adopt the same detailed practice. Such potential diversity of practice will require that designated competent authorities and SROs make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges to staff working to monitor compliance. The existence of good practice guidance, training, industry studies and other available information and materials will assist the designated competent authority or an SRO in determining whether a dealer in precious metals or a dealer in precious stones has made sound risk-based judgments.

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

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

Potential Benefits:

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

Potential Challenges:

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

Chapter Three: FATF and the Risk-Based Approach

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

38. The risk-based approach is either incorporated into the Recommendations (and the Methodology) in specific and limited ways in a number of Recommendations, or it is inherently part of or linked to those Recommendations. For instance, for DNFBPs, including dealers, risk is addressed in three principal areas (a) Customer Due Diligence (*R.5, 6, 8 and 9*); (b) businesses' internal control systems (*R.15*); and (c) the approach of oversight/monitoring of DNFBPs, including dealers (*R.24*).

Customer and counterparty due diligence (R. 5, 6, 8 and 9)

39. Risk is referred to in several forms:

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

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

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

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

Internal control systems (R.15)

40. Under Recommendation 15, the development of "appropriate" internal policies and 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 and counterparties, products and services, geographic areas of operation and so forth. The Interpretative Note to Recommendation 15 makes it clear that a country may allow DNFBPs, including dealers, to have regard to the money laundering and terrorist financing risks, and to the size of the business, when determining the type and extent of measures required.

Regulation and oversight by designated competent authorities or SROs (R.24)

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

Applicability of the risk-based approach to terrorist financing

42. There are both similarities and differences in the application of a risk-based approach to terrorist financing and money laundering. They both require a process for identifying and assessing risk. However, the characteristics of terrorist financing makes its detection difficult and the implementation of mitigation strategies may be challenging due to considerations such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

43. Funds that are used to finance terrorist activities may be derived from criminal activity or may be from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing, though the activity, which may be indicative of suspicion, may not be identified as or connected to terrorist financing. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal risk with regard to money laundering. Where funds are from legal sources it is even more difficult to determine if they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in

appearance, such as the purchase of materials and services to further their goals, with the only covert fact being the intended use of such materials and services purchased. Therefore, while terrorist funds may be derived from criminal activity as well as from 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 dealers to determine the type of underlying criminal activity, or intended terrorist purpose, rather the dealer's role is to identify and report the suspicious activity. The FIU and law enforcement authorities will then examine the matter further and determine if there is a link to terrorist financing.

44. The ability of dealers 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 on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering).

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

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

Limitations to the risk-based approach

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

48. Requirements to freeze assets of identified individuals or entities, in countries where such requirements exist, are independent of any risk assessment. The requirement to freeze is absolute and cannot be impacted by a risk-based process. Similarly, while the identification of potential suspicious transactions can be advanced by a risk-based approach, the reporting of suspicious transactions, once identified, is not risk-based. See paragraphs 132 and 133.

49. There are several components of customer and counterparty due diligence – identification and verification of the identity of customers and counterparties and their 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 and counterparties are requirements which must be completed regardless of the risk-based approach. However, in relation to all other CDD components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep

records and documents that have been obtained for due diligence purposes, as well as transaction records, is not dependent on risk levels.

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

51. Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk customers and counterparties, 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 and counterparties may only become evident once a relationship with a customer or counterparty has begun. This makes appropriate and reasonable monitoring of customer and counterparty 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 and counterparties will be monitored in exactly the same way. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this could be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption.

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

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

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

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

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

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

SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES

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

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

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

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

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

58. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of designated competent authorities or SROs and the nature of DNFBPs, including dealers, each country's judgements about the risks will be unique, as will their decisions about how to implement a national assessment in practice. A national assessment need not be a single formal process or document. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and current understanding of the risks. Designated competent authorities and SROs, in consultation with the private sector, should consider how best to achieve this while also taking into account any risk associated with providing information on vulnerabilities in their financial and non-financial systems to money launderers, terrorist financiers, and other criminals. Such consultation will be seen by such dealers as increasing their own knowledge of AML/CFT issues, as enhancing cooperation with the public sector, and as promoting consistency and a fair and level playing field within their industries.

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

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

60. The risk-based approach does not mean the absence of a clear statement of what is required from the DNFBPs, including dealers. However, under the risk-based approach, dealers should have a degree of flexibility to implement policies and procedures which respond appropriately to their own risk assessment. In effect, the standards implemented may be tailored and/or amended by additional measures as appropriate to the risks of an individual business. The fact that policies and procedures, in accordance to

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

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

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

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

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

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

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

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

Principle four: identifying the main actors and ensuring consistency

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

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

- Government – this may include legislature, executive, and judiciary.
- Law enforcement agencies - this might include the police, customs and similar agencies
- The financial intelligence unit (FIU), security services, other similar agencies.
- Designated competent authorities/SROs
- The private sector – this might include dealers' firms, national and international trade bodies and associations, financial institutions that specialize in these industries and businesses, 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 dealers' 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.

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

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

- Dealers 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 and counterparty due diligence.
- Acknowledging that a dealer's ability to detect and deter money laundering and terrorist financing may sometimes be necessarily limited and that information on risk factors is not always robust or freely available. There should therefore be reasonable policy and monitoring expectations about what a dealer in precious metals or a dealer in precious stones with good controls aimed at preventing money laundering and the financing of terrorism is able to achieve. A dealer may have acted in good faith to take reasonable and considered steps to prevent money laundering, and have documented the rationale for its decisions, and yet still be abused by a criminal.
- Acknowledging that not all high-risk situations are identical and as a result will not always require the application of precisely the same type of enhanced due diligence.

Principle five: information exchange between the public and private sectors

71. Effective information exchange between the public and private sectors will form an integral part of a country's strategy for combating money laundering and terrorist financing. In many cases, it will allow the private sector to provide designated competent authorities and SROs with information they identify as a result of previously provided government intelligence.

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

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

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

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

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

Chapter Two: Implementation of the Risk-Based Approach

Assessment of risk to inform national priorities

76. A risk-based approach should be built on sound foundations: effort must first be made to ensure that the risks are well understood. As such, a risk-based approach should be based on an assessment of the

threats. This is true whenever a risk-based approach is applied, at any level, whether by countries or individual firms. A country's approach should be informed by its efforts to develop an understanding of the risks in that country. This can be considered as a "national risk assessment".

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

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

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

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

80. The desired outcome is that decisions about allocating responsibilities and resources at the national level are based on a comprehensive and up-to-date understanding of the risks. To achieve the desired outcome, designated competent authorities and SROs should ensure that they identify and provide dealers with the information needed to develop this understanding and to design and implement measures to mitigate the identified risks.

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

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

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

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

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

Defining the acceptable level of risk

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

86. As described in Section One, all activity involves an element of risk. Designated competent authorities and SROs should not prohibit dealers from conducting business with high risk customers and counterparties as long as appropriate policies, procedures and processes to manage the attendant risks are in place. Only in specific cases, for example when it is justified by the fight against terrorism, crime or the implementation of international obligations, are designated individuals, legal entities, organisations or countries denied any access to services.

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

88. Designated competent authorities and SROs expect dealers to put in place effective policies, programmes, procedures and systems to mitigate risks, while acknowledging 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 the purpose of preventing dealers 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' or counterparty's business. This is why developing an accurate customer/counterparty 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 quickly limiting the utility of such typologies.

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

Proportionate monitoring actions to support the risk-based approach

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

91. In the course of their examinations, designated competent authorities and SROs should review a dealer'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 a dealer's business and the adequacy of its mitigation measures. Where available, assessments carried out by or for other dealers in precious metals and/or dealers in precious stones may be a useful source of information. The competent authority/SRO assessment of management's ability and willingness to take necessary corrective action is also a critical determining factor. Designated competent authorities and SROs should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider

consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe supervisory or monitoring response.

92. Nevertheless, it may happen that the lack of detection of an isolated high risk transaction, or of transactions of an isolated high risk customer, will in itself be significant, for instance where the amounts are significant, or where the money laundering and terrorist financing typology is well known, or where a scheme has remained undetected for a long time. Such a case might indicate an accumulation of weak risk management practices or regulatory breaches regarding the identification of high risks, monitoring, staff training and internal controls, and therefore, might alone justify action to ensure compliance with the AML/CFT requirements.

93. Designated competent authorities and SROs can and should use their knowledge of the risks associated with products, services, customers and counterparties, and geographic locations to help them evaluate a dealer's money laundering and terrorist financing risk assessment, with the understanding, however, that they may possess information that has not been made available to the dealer and, therefore, the dealer would not have been able to take such information into account when developing and implementing a risk-based approach. Designated competent authorities and SROs (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist dealers in managing their risks. Where dealers are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by their designated competent authorities and SROs[2]. Guidance designed for dealers is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where the dealers use excessively narrow risk categories that do not capture all existing risks, or adopt criteria that lead to the identification of a large number of higher risk relationships, but without providing for adequate additional due diligence measures.

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

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

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

a) Regulatory Transparency

97. In the implementation of proportionate actions, regulatory transparency will be of paramount importance. Designated competent authorities and SROs are aware that dealers, while looking for operational freedom to make their own risk judgments, will also seek guidance on regulatory obligations. As such, the designated competent authority/SRO with AML/CFT monitoring responsibilities should seek to be transparent in setting out what it expects, and will need to consider appropriate mechanisms of

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

communicating these messages. For instance, this may be in the form of high-level requirements, based on desired outcomes, rather than detailed process.

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

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

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

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

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

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

- The quality of internal procedures, including ongoing employee training programmes and internal audit, compliance and risk management functions.
- Whether or not the risk management policies and processes are appropriate in light of the dealers' risk profile, and are periodically adjusted in light of changing risk profiles.
- The participation of senior management to confirm that they have undertaken adequate risk management, and that the necessary procedures and controls are in place.

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

Chapter One: Risk Categories

103. In order to implement a reasonable risk-based approach, dealers in precious metals/dealers in precious stones should identify the criteria to assess potential money laundering and terrorist financing risks. These risks will vary according to the activities undertaken by the dealers.

104. Identification of the money laundering and terrorist financing risks, to the extent that the terrorist financing risk can be identified, will allow dealers in precious metals/dealers in precious stones to determine and implement proportionate measures and controls to mitigate these risks.

105. Money laundering and terrorist financing risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling dealers in precious metals/dealers in precious stones 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 dealer to another, depending upon their respective circumstances. Consequently, dealers in precious metals/dealers in precious stones will have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a dealer's discretion.

106. While there is no agreed upon set of risk categories for dealers in precious stones/dealers in precious metals, the examples provided herein are the most commonly identified risk categories. There is no single methodology for applying these risk categories. However, the application of these risk categories is intended to assist in designing an effective strategy for managing the potential risks.

Country/Geographic risk

107. There is no universally agreed definition by either designated competent authorities, SROs, or dealers that prescribes whether a particular country or geographic area (including the country within which the dealer 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 the determination that a country poses a higher risk are set out below.

108. Some countries and geographic locations are of greater AML/CFT concern, and the risk level can rise or lower dependent upon the country of any of the elements of a transaction, including (1) where a product is mined; (2) where a product is refined or finished; (3) location of a seller; (4) location of a purchaser; (5) location of the delivery of a product and (6) location of funds being used in the transaction.

Background information box

Geographic risk – where a product is mined. Mining can be vulnerable to terrorist financing if it occurs in remote locations with minimal governmental presence or infrastructure. In some areas, for example, gold mining can be dominated by armed non-governmental groups.

Mining for jewels is also geographically widespread, and sometimes occurs in areas of significant turmoil. Unlike diamond mining, mining for jewels is largely small and informal, carried on by local prospectors and owners in alluvial sources, very few of which, if any, are publicly traded companies. Some mines are government owned, and mines often have licenses issued by government agencies involved with natural resources, but even such mines are often remote from strong governmental oversight, and often in areas of substantial conflict and crime, including terrorism. Buyers travel to the mines or to nearby communities and buy jewels, sometimes in a manner controlled by government, sometimes either directly from miners or from local intermediaries. Because many of these areas do not have reliable financial systems, payments are often in cash and informal, or are made through third party accounts, again increasing risk.

109. Factors that should be considered in a determination that a country may or may not pose a higher risk with regard to a proposed transaction in diamonds, jewels or precious metals include:

- For rough diamonds, whether a producing or trading country participates in the Kimberley Process.
- Whether there is known mining or substantial trading of the transaction product – diamonds, jewels or precious metals - in a transaction source country.
- Whether a country would be an anticipated source of large stocks of existing diamonds, jewels or precious metals, based upon national wealth, trading practices and culture (centres of stone or jewel trading, such as Antwerp, Belgium) or unanticipated (large amounts of old gold jewellery in poor developing countries). It should be recognized, however, that gold and silver have cultural and economic significance in a number of developing countries, and very poor people may have, buy and sell these metals.
- The level of government oversight of business and labour in mining and/or trading areas.
- The extent to which cash is used in a country.
- The level of regulation of the activity.
- Whether informal banking systems operate in a country, *e.g.* hawalas operate in many developing countries.
- Whether designated terrorist organisations or criminal organisations operate within a country, especially in small and artisan mining areas.
- Whether there is ready access from a country to nearby competitive markets or processing operations, *e.g.* gold mined in Africa is more frequently refined in South Africa, the Middle East or Europe rather than in the United States, and a proposal to refine African gold in the United States would be unusual and higher risk.
- Whether, based on credible sources3, appropriate AML/CFT laws, regulations and other measures are applied and enforced in a country.

[3] "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by

- The level of enforcement of laws addressing corruption or other significant organized criminal activity.
- Whether sanctions, embargoes or similar measures have been directed against a country.

Customer and counterparty risk

Retail Customer Risk

110. A retail customer of precious metals or precious stones will, in general, not have a business purpose for a purchase of an article of jewellery, a precious stone of a precious metal. A purchase is likely to be made for purely personal and emotional reasons that cannot be factored into an AML/CFT risk assessment. Higher risk can be seen, however, in certain retail customer transaction methods:

- Use of cash. It should be recognized, however, that many persons desire anonymity in jewellery purchases for purely personal reasons, or at least the absence of paper records, with no connection to money laundering or terrorist financing.
- Payment by or delivery to third parties. However, not all third party payments are indicative of AML/CFT. It is relatively common in jewellery purchases that a woman will select an article of jewellery, and a man will later make payment and direct delivery to the woman.
- Structuring.

Business Counterparty Risk

Background information box

There are many different stages and transactions and counterparties involved in the precious stones and precious metals businesses. As set forth above, miners range from international companies to individuals. Intermediaries may be well established local buyers from miners, or itinerant foreign buyers, or hawalas. Retail jewellers may buy articles of used jewellery, as may direct buyers and pawnshops. Each of these businesses may present a money laundering risk. Dealers may buy from or sell to other counterparties who also work in their precious metals or precious stones businesses, or sell to the public through retail sales (which may often be anonymous). Dealers will need to consider the risks associated with each stage at which they participate. A risk based approach should account for higher risk customers and counterparties at every stage.

Apart from the retail sector, trade in diamonds, jewels and precious metals is traditionally private, as a matter of commercial protection or security. Dealers have traditionally protected their counterparties, their materials, and their business practices from public knowledge, in the interest of protecting themselves from criminal activity, and from potential independent interaction by competitors with their customers and counterparties or suppliers. However, it is necessary for dealers themselves to know that they are dealing with legitimate counterparties.

In some sectors within precious metals and precious stones businesses, trust based on personal contact is an essential element of conducting business, and such trust and personal contact assist in lowering counterparty risk. In addition, each industry has trade resources, such as trade associations and directories, with which to establish some background and credit information and these should be consulted. Checks must be made upon any new counterparty that is unknown to a dealer, and particularly if also unknown within the dealer's industry. A counterparty, who proposes a transaction in diamonds, jewels or precious metals should have the knowledge, experience and capacity, financial and technical, to engage in that transaction.

---

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.

111. Higher risk counterparties include a person who:

- Does not understand the industry in which he proposes to deal, or does not have a place of business or equipment or finances necessary and appropriate for such engagement, or does not seem to know usual financial terms and conditions.
- Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
- Has significant and unexplained geographic distance from the dealer in precious metals or dealer in precious stones.
- Uses banks that are not specialised in or do not regularly provide services in such areas, and are not associated in any way with the location of the counterparty and the products.
- Makes frequent and unexplained changes in bank accounts, especially among banks in other countries.
- Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose.
- Will not identify beneficial owners or controlling interests, where this would be commercially expected.
- Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries, see the paragraph above.
- Uses cash in its transactions with the dealer in precious metals or dealer in precious stones, or with his own counterparties in a nonstandard manner.
- Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
- Is a politically exposed person (PEP).

Product/Service Risk

112. An overall risk assessment should also include a determination of the potential risks presented by products and services offered by a dealer in precious metals or a dealer in precious stones. The determination of risks of products and services should include a consideration of the following factors:

(a) Products offered

113. All diamonds, jewels, and precious metals can potentially be used for money laundering and terrorist financing, but the utility and consequent level of risk are likely to vary depending on the value of the product. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. However, dealers must be aware that values can be volatile dependent upon supply and demand. Relative values of some materials can vary dramatically between different countries, and over time.

114. Dependent upon the nature of the transaction, counterparties, and quantities, gold can be higher risk. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself, *e.g.* by hawalas. Gold is available in a variety of forms, e.g. bars, coins, jewellery, or scrap, and trades internationally in all of these forms.

115. Although scrap gold alloys or other gold-bearing scrap may require substantial processing and refining to reach an end market, the costs will be discounted in advance, and the scrap may still trade for high value in multi-billion dollar worldwide markets. Values of many scrap materials are uncertain and not precisely knowable until they have been processed and assayed, which can present an AML risk if the parties undervalue or overvalue international shipments.

116. Alluvial gold and gold dust can be indicative of informal mining by individuals and small groups, often in areas that are characterized by informal banking and absence of regulation, and so may be higher risk.

117. The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering. For example, diamonds are small, light in weight, not detected by metal detectors, and a very large value can be easily concealed.

118. Finally, the risk of dealing in stolen or fraudulent products must be taken into account. As with all valuable objects, diamonds, jewels and precious metals are attractive to thieves, and dealers must be aware of the risks of trading in stolen products. For example, jewellery dealers, pawn shops and buyers of used gold jewellery should remain alert to the possibility of being offered stolen jewellery. In addition to stolen goods, dealers should be aware of the risks associated with fraudulent goods, such as synthetic diamonds represented as natural diamonds, or 14 karat gold represented as 18 karat.

(b) Services offered

119. Major gold dealers create metal accounts for their customers, for temporary secure storage or for investment, and they transfer counterparties' gold credits in these accounts among themselves, and among repositories and delivery destinations worldwide, with services comparable to those provided by banks with money and financial credits. Such services, by banks as well as by major gold dealers, may be useful to money launderers and terrorist financiers to move high values through international commerce, under the guise of legitimate business, but are unlikely to be anonymous and irregular, and thus may be of lower risk.

(c) Market characteristics

120. It is helpful to bear in mind the following broad principles which may lower the risk levels of particular transactions:

- Limited resale opportunities – limited resale opportunities are likely to be unattractive to money launderers[4].
- Size of market – a small market is likely to make it more difficult for a money launderer to structure transactions, to layer multiple transactions (to create distance between the seller and the ultimate purchaser), and to conduct anonymous transactions, and will thus be less attractive to money launderers.
- Degree of expertise required – if specialized expertise is required for transactions, risk of use of such transactions by money launderers may be lower. For example, diamonds are unique

[4] For example, spent industrial catalysts that contain platinum group metals generally have resale opportunities limited to platinum refiners, and thus are of lower risk in money laundering. Silver used in imaging and electronics, which are specialized applications from which value is not easily removed, is similarly of lower risk. Platinum and silver jewellery and coins could, of course, be used by money launderers. Silver has been used for centuries as money, as has special prominence in some geographical areas and cultures, *e.g.* India.

objects, some with extremely high value, some with much less, all dependent upon size and physical characteristics, usually as judged by persons with expertise in diamond evaluation. As transaction values increase, either because of higher numbers of diamonds involved or higher quality of individual diamonds, so does the need for expertise and specialized markets increase. Money launderers may not have such expertise. Such expertise exists, however, in many places, and money launderers may be able to obtain it, or to employ it.

- Degree of market regulation – if a market is regulated, depending upon the degree of regulation, transactions in that market may be lower risk (see below the other variables to take into account for the determination of risks).
- Transaction costs – money laundering and terrorist financing can involve multiple transactions, with criminals first placing illegal assets within a legitimate product, as anonymously as possible, then layering those assets through intermediate transactions, and then removing them at a different time and place. Money launderers want to get as much as possible of their illegal assets out of these transactions. They may be prepared to accept losses in these layering transactions, but may prefer to keep them to a minimum. Therefore transactions involving high value product and low transaction costs may be particularly attractive to money launderers and terrorist financiers. For example, a purchase of pure gold coins, and subsequent sale of those coins at another location, will quickly return most of the original purchase price. On the other hand a purchase of a specialty gold alloy may have a resale value of only the gold content, losing any value added in manufacturing, and losing gold refining charges as well. Such a transaction will cause a money launderer to pay substantial transaction costs and may therefore be lower risk.

(d) Financing methods

121. The method of payment used affects the risk of money laundering and terrorist financing taking place. The risks are likely to be reduced if transactions take place through the mainstream banking system. Conversely, the risk may increase in the following situations:

- Cash, especially in large amounts, can be a warning sign, especially if the use of cash is anonymous or intentionally hides an identity, *e.g.* the true purchaser funds the transaction by giving cash to a third party, who then becomes the nominal and identified purchaser.
- Payments or delivery of product to or from third party accounts, *e.g.* accounts in the names of persons other than approved counterparties.
- Payments to or from accounts at financial institutions that are unrelated to a transaction or approved counterparties, such as banks located in countries other than the location of the counterparty or transaction.
- Non-bank financial mechanisms such as currency exchange businesses or money remitters.

<u>Variables that may change risk determination</u>

122. To design a risk-based approach methodology, there may be a need to look at a series of other variables that may increase or decrease the perceived risk posed by a particular customer or transaction:

- The level of effective AML/CFT regulation or other oversight or governance regime to which a counterparty is subject. A counterparty that is a dealer in precious metals or a dealer in precious stones operating in a country under a robust AML/CFT regime, or a system such as the Kimberley Process, poses less risk from a money laundering perspective than a counterparty that is unregulated or subject only to minimal AML regulation. To be given such

a lower risk consideration, a counterparty should have a compliance program and certify to compliance with its applicable regulatory system.

Background information box

The type and level of regulation varies greatly among the different types of precious metals and precious stones. For example, in some countries, dealers are required to have a government issued license for their particular businesses, in others they are not. There may be no or limited regulation when a product is mined and sold for the first time, but the level of regulation may increase as the product continues to be traded.

Some governments are also involved in transactions through export and import regulatory systems, often for the purpose of collecting taxes or duties, which require traders to describe their materials and declare values and counterparties of export or import. Such government involvements may lower risk, but may vary from country to country, and impacts upon risk must be evaluated directly by a dealer in precious metals or a dealer in precious stones.

There is some government regulation of precious metals trading, but most transactions are not conducted in regulated markets. Gold is traded worldwide in very large amounts in direct physical transactions and through financial derivatives, *i.e.* forwards and futures, which can be used to acquire and sell rights in physical gold stocks. Such paper gold transactions, of any size, are highly unlikely to be anonymous or conducted in cash, certainly in regulated markets and probably in unregulated markets, but should not be ignored for anti money laundering purposes.

A large proportion of rough diamond sales are made through Belgium, which strictly regulates dealers and transactions (including the physical inspection and value assessment of all imported and exported diamonds, hence for instance excluding valuation and synthetic diamonds related risks), and through bourses with stringent membership rules of practice. Some countries participate in the Kimberley Process. The Kimberley Process applies to dealers in rough diamonds, including importers and exporters of rough diamonds, when they operate in participant countries. When it applies the Kimberly Process significantly lessens the ML/TF risk level. Systems of dealer warranties and transactions through bourses further reduce risk in the trade of polished diamonds and jewellery containing diamonds, as do dealings with only bank transfer payments among regulated and government supervised dealers.

- The size of the transaction, with larger transactions presenting higher risk, always bearing in mind the possibility of deliberate structuring of smaller transactions.
- The level of government regulation of counterparty's business and accounting practices. Companies and their wholly owned subsidiaries that are publicly owned and traded on a regulated exchange, or that have publicly issued financial instruments, generally pose minimal money laundering risks. Note however that this is not always so, and publicly traded companies may be established by money launderers[5].
- Government trade flow inspection mechanisms that involve physical inspections, trade flow follow up and/or valuation verifications. In general, if a government has developed a gate keeper role that monitors incoming and/or outgoing trade flows, including physical inspection of goods and value assessments, the money laundering risk may be considerably reduced, as well as risks related to the use of synthetic diamonds.
- The nature and extent of banking involvement. In general, a lower risk level is present where a transaction is entirely financially settled, both at the side of the dealer and the counterparty, through a banking institution that is situated in an FATF member country and that is known to be actively involved in payment flows and financing arrangements in the particular trade, provided the transaction is generally routine (including payment that closely follows routine trade flows) and that the documentation contains adequate identification of all parties concerned (see also the risk attached to financing methods above).

[5] See FATF Report on Money Laundering Typologies, 2002-2003, paragraph 37; Example 10: Listed legal entity created specifically for laundering illegal funds; Example 12: Narcotics trafficker takes control of a publicly traded company.

- The regularity or duration of the business relationship, or of general knowledge of the counterparty's role in the industry. Longstanding relationships involving frequent contact provide an understanding of a counterparty's legitimacy within the dealer's industry, and information by which a proposed transaction can be evaluated for consistency with industry norms.
- The familiarity of a dealer in precious metals or a dealer in precious stones with a counterparty's country, including knowledge of applicable local laws, regulations and rules, as well as the structure and extent of regulatory oversight.

Controls for higher risk situations

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

- General training for appropriate personnel on money laundering and terrorist financing methods and risks relevant to dealers.
- Targeted training for appropriate personnel to increase awareness of higher risk customers or transactions.
- Increased levels of know your customer/counterparty (KYC) or enhanced due diligence.
- Escalation within dealer management required for approval.
- Increased monitoring of transactions.
- Increased controls and frequency of review of relationships.

Chapter Two: Application of a Risk Based Approach

124. A risk-based approach should be applied across the full breadth of an enterprise, including a multinational enterprise. Policies, standards and procedures should be similar, if not identical across an enterprise or business, and separate parts of an enterprise or a business should communicate with each other regarding the implementation of their AML/CFT program. If a person or transaction is classified in a high risk category in one part of an enterprise, the other parts of that enterprise that might encounter such person or transaction need to be advised at the same time.

125. Legal standards and enforcement cultures vary, and persons engaged in business in a country must be aware of and respond to that country's laws and competent authorities. There should be similarity along the following common implementation steps:

Customer due diligence/Know your counterparty/Customer

126. The Identify Your Counterparty/Customer activity within a dealer's AML/CFT program is intended to enable the dealer in precious metals or the dealer in precious stones to form a reasonable belief that it knows the true identity of each counterparty/customer and the types of transactions the counterparty proposes. A dealer's program should include procedures to:

- Identify and verify counterparties/customers before establishing a business relationship, such as entering into contractual commitments. This identified natural or legal person or authorized

and fully identified agents should then be the only person or persons to whom payment is authorized to be made, or product delivered, unless legitimate and documented business reasons exist, and any third party is appropriately identified and its identity verified.

- Identify beneficial owners and take reasonable measures to verify the identities, such that the dealer is reasonably satisfied that it knows who the beneficial owners are. The measures which have to be taken to verify the identity of the beneficial owner will vary depending on the risk. For legal persons and arrangements this should include taking reasonable measures to understand the ownership and control structure of the counterparty/customer.
- Obtain information to understand the counterparty's/customer's circumstances and business, including the expected nature and level of proposed transactions.

127. In the circumstances where the FATF Recommendations are applicable (*i.e.* for transactions involving cash equal to or above USD/EUR 15 000), the general rule is that counterparties/customers must be subject to the full range of CDD measures. Furthermore, additional Identify Your Counterparty/Customer activity and procedures should be applied to higher risk determinations (such as PEPs or transactions involving higher risk countries). In these cases, for instance, a dealer in precious metals or a dealer in precious stones should implement additional measures and controls to mitigate that risk. Such measures may include increased levels of know your counterparty or enhanced due diligence and greater direct contact with a counterparty (for example, observing its operations, personnel and equipment, would provide additional verification of its legitimacy). It will also require increased monitoring of transactions.

128. These steps should be recorded and maintained in a file regarding each counterparty/customer. In circumstances defined by the public authorities where there are lower money laundering or terrorist financing risks, dealers may be allowed to apply reduced or simplified CDD measures when identifying and verifying the identity of the counterparty/customer and the beneficial owner having regard to the type of counterparty/customer, product or transaction.

129. In other circumstances (*i.e.* for transactions not involving cash equal to or above USD/EUR 15 000) and where national law does not require otherwise, counterparty/customer identification can, however, be accomplished through broader industry practices and associations that already maintain comparable data to which the authorities have ready access, or by reference to government held databases (registered dealer database, VAT related database, etc.). This will reduce transaction burdens, particularly upon small and mid-size dealers who already rely upon such industry resources to maintain security and high standards in their business practices. For example, in the diamond industry, transactions for rough diamonds are conducted within the scope of the Kimberley Process. Trading in rough diamonds and polished diamonds can occur through bourses that are members of the World Federation of Diamond Bourses. Dealers might transparently reference these sources of counterparty/customer identification rather than recreate all identification data in multiple dealer and transaction files.

130. In similar circumstances, other regulatory programs and/or industry associations may provide similar counterparty information and assurances. Transactions with well-known, longstanding counterparties might also be identified by transparent reference to existing information of a dealer, rather than be recreated. Such streamlined counterparty identification practices should, of course, be limited to transactions with standard trading and bank payment practices that do not give rise to suspicion and concern, and do not in any case fully eliminate the need to apply risk based analysis to transactions, customers, or counterparties.

Monitoring of counterparties/Customers and transactions

131. The degree and nature of monitoring by a dealer in precious metals or a dealer in precious stones will depend upon the size of the business and the risk assessment that the dealer has made. Based on such risk assessment and in accordance with any legislative or regulatory requirements, not all transactions or counterparties/customers will be monitored in the same way and to the same degree. A risk may only become evident once a counterparty has begun transactions, particularly if such transactions differ from those originally anticipated, and changes in transactions should be noted and evaluated. A monitoring program and results of monitoring should always be documented, and a dealer in precious metals or a dealer in precious stones should periodically assess its monitoring program for adequacy.

Suspicious transaction reporting

132. The circumstances that will trigger a requirement to report a suspicious transaction or activity to a dealer's competent authority are usually rules-based and set forth in national law, and a risk-based approach for such reports is not applicable. An AML/CFT program that is founded on the risk-based approach will, however, direct attention and resources toward higher risk activities, will more readily identify suspicious activity, and should encourage reporting of suspicious activity.

133. The adequacy of a dealer's AML/CFT program to identify and properly report suspicious activity should be periodically reviewed.

Counter financing of terrorism

134. Dealers should make reference to paragraphs 42 to 46 in relation to terrorist financing.

Training and awareness

135. The success of a dealer's AML/CFT program will depend upon its application throughout the full range of the dealer's business activities, and thus upon appropriate training of employees. A dealer should inform all employees that it has an AML/CFT program designed and intended to detect and deter money laundering and terrorist finance, and that their awareness and participation are important. All employees should be encouraged and trained to contact management regarding suspicious activity that they observe or of which they become aware.

136. Training of specific employees will vary according to their roles, *e.g.* counterparty/customer contact, receiving and inspection, trading, banking, accounting, IT, and according to the levels of risk associated with counterparties/customers and transactions with which they have a business association. This training should be periodically reviewed for adequacy and repeated as appropriate. Each AML/CFT incident or inquiry arising in the course of business should also be used as an opportunity to reinforce the awareness and understanding of employees regarding a dealer's AML/CFT program and their roles in implementation of that program. If circumstances of suspicion, concern or higher risk are revealed in monitoring, additional training should be specifically directed to those circumstances with appropriate employees.

Chapter Three: Internal Controls

137. Many DNFBPs differ significantly from financial institutions in terms of size. By contrast to most financial institutions, a significant number of DNFBPs have only a few staff. This limits the resources that small businesses and professions can dedicate to the fight against money laundering and terrorist financing. For a number of DNFBPs, a single person may be responsible for the functions of front office, back office, money laundering reporting, and senior management. This particularity of DNFBPs, including

dealers, should be taken into account in designing a risk-based framework for internal controls systems. The Interpretative Note to Recommendation 15, dealing with internal controls, specifies that the type and extent of measures to be taken for each of its requirements should be appropriate having regard to the size of the business.

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

Culture of compliance

139. This should encompass:

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

Senior management ownership and support

140. A risk-based AML/CFT program requires commitment, participation and authority of owners and controlling persons. It should be part of a culture of legal and ethical compliance that these senior management officials should inculcate to all employees, and to counterparties, and to other persons associated with the business.

141. The nature and extent of AML/CFT controls will depend upon a number of factors including:

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

142. A risk-based AML/CFT program should be established and implemented in coordination with other business compliance and security programs. Verification of employees, for example, through background and security screening can be cross-checked with AML/CFT verification of customers and counterparties. Daily checks of inventories by independent groups within a company to dissuade and minimize theft losses can also inform an AML/CFT program of suspicious activity.

143. A risk-based AML/CFT program requires specialized expertise about a dealer's industry, about a dealer's particular business within that industry, and about particular counterparties. It also requires knowledge of money laundering techniques, and how they might be used within particular industry transactions and areas of operation. Within many small, privately held and family businesses in these

industries, all of these skills and authorities are available primarily, or only, at the level of ownership/senior management. Within larger enterprises, a person with these skills will need to be designated and authorized as a Compliance Officer.

144. A designated Compliance Officer should have a reputation within the dealer's enterprise for integrity and sound judgment, should be authorized and willing to contradict persons with more limited interests in proposed transactions and counterparties, including the owners, and should be known within a dealer's enterprise as such a person.

145. Having regard to the ML/TF risks and the size of the dealer, a dealer's AML/CFT internal control programme should include procedures that:

- Ensure that regulatory record keeping and reporting requirements are met, and that changes in regulatory requirements are incorporated[6].
- Implement risk-based counterparty due diligence procedures.
- Provide for adequate controls for higher risk counterparties, transactions and products.
- Enable the timely identification of reportable transactions and ensure accurate filing of required reports.
- Provide for adequate monitoring.
- Provide for adequate supervision of employees.
- Provide for appropriate and updated training.

146. An AML/CFT program should be a living document, changing as new circumstances arise, adapting to increased understanding of its elements, such as information derived from periodic review, monitoring and suspicious activity, and responding to recommendations. Dealers should also take account of relevant material published by designated competent authorities and SROs.

147. Senior management and its designated Compliance Officer should also arrange for regular periodic review of the AML/CFT program and its operation, for implementation of recommendations arising from such review, and for ongoing improvement of the program. Such review need not be by persons outside of a dealer's business, but should be by a qualified person who, if practicable, is independent of the Compliance Officer. A person who is not directly involved in the day-to-day operation of the AML/CFT program will bring a fresh view to program activities. In small and mid size companies where ownership/senior management is directly involved in the AML/CFT program, periodic review need not be as formal an undertaking. If a dealer reports transactions to designated competent authorities or SROs, and receives appropriate feedback from such authorities, written reports of this regulatory activity may serve as such review or as a database for it.

148. Senior management not directly associated with the AML/CFT program should be briefed upon its operations and lessons learned from experience, and should be asked for questions and comments. This cross-fertilization will both strengthen the program, and further inculcate its principles within the enterprise or business.

---

[6] Application of an AML/CFT Program is not complete without documentation of such application. Documentation requires systematic analysis, which is the foundation of a risk-based approach. It also provides an institutional memory of that analysis, and its determinations and actions. It facilitates information sharing within a dealer's enterprise, and, when appropriate, with competent authorities. And it provides a basis upon which an AML/CFT program and practices can be measured and improved.

ANNEXES

ANNEX 1 – SOURCES OF FURTHER INFORMATION

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

A. Financial Action Task Force Documents

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

http://www.fatf-gafi.org

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

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

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

- Mutual evaluation reports issued by FATF Style Regional Bodies:

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

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

3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
http://www.coe.int/moneyval
4. Eurasian Group (EAG)
http://www.eurasiangroup.org/index-7.htm

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

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

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

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

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

ANNEX 2 – GLOSSARY OF TERMINOLOGY

Beneficial Owner

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

Competent authorities

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

Counterparty

A person, entity or party engaged in the purchase and/or sale of precious metals or precious stones with other dealers of precious metals or precious stones, including both suppliers and retail customers.

Country

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

Designated Non-Financial Businesses and Professions

a. Casinos (which also includes internet casinos).

b. Real estate agents.

c. Dealers in precious metals.

d. Dealers in precious stones.

e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons.

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

FATF Recommendations

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

Identification data

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

Politically Exposed Persons (PEPs)

Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Self-regulatory organisation (SRO)

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

ANNEX 3 – MEMBERS OF THE ELECTRONIC ADVISORY GROUP

FATF and FSRB members and observers

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

Dealers in precious metals and dealers in precious stones industries

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

Real estate industry

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

Trust and company service providers industry

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

Accountants industry

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

Casinos industry

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

Lawyers and notaries

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