



**Financial Action Task Force**  
Groupe d'action financière

**RBA GUIDANCE FOR CASINOS**

23 October 2008

**© FATF/OECD 2008**

**All rights reserved. No reproduction, copy, transmission or translation of this publication may be made without written permission.**

**Applications for permission to reproduce all or part of this publication should be made to:  
FATF Secretariat, OECD, 2 rue André Pascal 75775 Paris Cedex 16, France**

## TABLE OF CONTENTS

|   |    |
|---|----|
| SECTION ONE: USING THE GUIDANCE - PURPOSE OF THE RISK-BASED APPROACH.....   | 4  |
| Chapter One: Background and Context .....   | 4  |
| Chapter Two: The Risk-Based Approach – Purpose, benefits and challenges .....   | 6  |
| Chapter Three: FATF and the Risk-Based Approach.....  | 9  |
| SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES.....   | 14 |
| Chapter One: High-level principles for creating a risk-based approach .....   | 14 |
| Chapter Two: Implementation of the Risk-Based Approach.....   | 18 |
| SECTION THREE: GUIDANCE FOR CASINOS ON IMPLEMENTING THE RISK-BASED APPROACH.....  | 23 |
| Chapter One: Risk Categories.....   | 23 |
| Chapter Two: Application of a Risk Based Approach.....  | 30 |
| Chapter Three: Internal controls .....  | 33 |
| ANNEXES .....   | 35 |
| ANNEX 1 – SOURCES OF FURTHER INFORMATION .....  | 35 |
| A. Financial Action Task Force Documents .....  | 35 |
| B. Other sources of information to help assist countries and casinos risk assessment of countries and cross-border activities ..... | 35 |
| ANNEX 2 – GLOSSARY OF TERMINOLOGY.....  | 37 |
| ANNEX 3 – MEMBERS OF THE ELECTRONIC ADVISORY GROUP.....   | 39 |

## 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 Evaluation 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 casinos<sup>1</sup> was presented to the WGEI. After further international consultation with both public and private sectors, the FATF adopted this guidance at its October 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.

<sup>1</sup> All FATF references to “casinos” include Internet casinos.

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

Target Audience, Status and Content of the Guidance:

8. This guidance is presented in a way that is focused and relevant for casinos. The roles and therefore risks of the different DNFBP sectors are usually separate. However, in some business areas, there are inter-relationships between different DNFBP sectors, and between the DNFBPs and financial institutions. For example, some land-based casinos provide services similar to those provided by financial institutions, and Internet casinos tend to only make/receive payments using accounts held by financial institutions.

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

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

11. Recommendation 12 mandates that the requirements for customer due diligence, record-keeping requirements, and paying attention to all complex, unusual large transactions set out in Recommendations 5, 6, and 8 to 11 apply to casinos when their customers engage in financial transactions equal to or above USD/EUR 3 000.

12. Recommendation 16 requires that FATF Recommendations 13 to 15 regarding reporting of suspicious transactions 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 casinos.

13. Recommendation 24 requires that countries ensure that a designated competent authority has responsibility for the AML/CFT regulatory and supervisory regime for casinos. The competent authority should have adequate powers to perform its functions, including adequate powers to monitor and sanction. Casinos must also be licensed by a designated competent authority, who must take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest in, holding a management function in, or being an operator of a casino.

14. The wider audience for this guidance includes countries and regulators which are considering how to apply AML/CFT measures to casinos. Countries need to identify the most appropriate regime, tailored to address individual country risks, and which take into consideration the idiosyncrasies and activities of casinos and the other DNFBP sectors in their country. This regime should recognise the

differences between the DNFBP sectors, as well as the differences between the DNFBPs and financial institutions. However, this guidance does not override the purview of national authorities.

#### Observation on the particular activities carried out by casinos

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

16. Land-based casinos vary in a number of key areas which may impact upon money laundering or terrorist financing risk, *e.g.* types of gambling offered; location, speed and volume of business; types of payment, and payment methods, accepted from customers; size of premises; customers (regular customers with membership rules or passing trade such as casual tourists or organised casino tours); whether the casino owner forms part of a larger organisation owned by the same operator, and the general regulatory environment that the casino operates within.

17. Internet casinos also vary, *e.g.* whether the operator has other web sites, or whether an operator's server is in a different country from other parts of its business. These differences contribute to significant differences between land-based and internet casinos in a number of key areas, including customer contact.

18. Casinos are generally subject to a range of regulatory requirements, commercial considerations, and security measures, which can complement AML and CFT measures:

- Age verification.
- Financial crime controls.
- Social responsibility provisions.
- Security controls.
- Gaming surveillance, *e.g.* to deal with problem gambling.

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

### The purpose of the Risk-Based Approach

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

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

21. A number of the DNFBP sectors, including casinos, are already subject to regulatory or professional requirements which complement AML/CFT measures, *e.g.* in some countries casinos will be licensed and some of their activities will be overseen by government agencies. Where possible, it will be beneficial for casinos to devise their AML/CFT policies and procedures in a way that harmonises with

other regulatory or professional requirements. A risk-based AML/CFT regime should help ensure that the honest customers can access the services provided by casinos, but creates barriers to those who seek to misuse these services.

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

23. The strategies to manage and mitigate the identified money laundering and terrorist financing risks 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.

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

25. 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.

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

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

28. 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, 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, law enforcement or judicial authorities should take action as necessary and appropriate.

## Potential Benefits and Challenges of the Risk-Based Approach

### *Benefits:*

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

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

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

### *Challenges:*

32. A risk-based approach is not necessarily an easy option, and there may be challenges to overcome when implementing the necessary measures. Some challenges may be inherent to the use of the risk-based approach. Others may stem from the difficulties in making the transition to a risk-based system. A number of challenges, however, can also be seen as offering opportunities to implement a more effective system. The challenge of implementing a risk-based approach with respect to terrorist financing is discussed in more detail at paragraphs 44 to 48 below.

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

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

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

36. Designated competent authorities should place greater emphasis on whether a casino has an effective decision-making process with respect to risk management, and sample testing should be used or individual decisions reviewed as a means to test the effectiveness of a casino's overall risk management. Designated competent authorities should recognise and appreciate 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. Designated competent authorities may also wish to consider whether there is a demonstrated culture of AML/CFT compliance within a casino.

37. In implementing the risk-based approach, casinos should be given the opportunity to make reasonable judgements with respect to their particular situations. This may mean that no two casinos are likely to adopt the same detailed practices. Such potential diversity of practice will require that designated competent authorities 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 in determining whether a casino has made sound risk-based judgements.

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

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

Potential Benefits:

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

Potential Challenges:

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

### **Chapter Three: FATF and the Risk-Based Approach**

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

40. 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 casinos, 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 casinos (R.24).

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

41. Risk is referred to in several forms:

- a) Higher risk – Under Recommendation 5, a country must require its DNFBPs, including casinos, to perform enhanced due diligence for higher-risk customers, business relationships or transactions. Recommendation 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 casinos, to take lower risk into account in deciding the extent of the CDD measures they will take (see Methodology criteria 5.9). Casinos 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 casinos, to give special attention to the risks arising from new or developing technologies that might favour anonymity.
- d) Risk assessment mechanism – The FATF standards expect that there will be an adequate mechanism by which competent authorities assess or review the procedures adopted by casinos to determine the degree of risk and how they manage that risk, as well as to review the actual determinations themselves. This expectation applies to all areas where the risk-based approach applies. In addition, where the competent authorities 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)*

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

#### *Regulation and oversight by competent authorities (R.24)*

43. Countries should ensure that casinos are subject to comprehensive regulatory and supervisory regime that ensures they are effectively implementing the AML/CFT requirements. Countries may have regard to the risk of money laundering or terrorist financing when determining the extent of measures to supervise casinos for AML/CFT purposes. If there is a proven low risk then lesser measures may be taken.

#### Applicability of the risk-based approach to terrorist financing

44. 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.

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

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

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

48. 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 casinos, 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

49. 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.

50. 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 paragraph 131.

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

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

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

#### Distinguishing Risk-Based Supervision and Risk-Based Policies and Processes

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

55. However, it should also be noted that the risk factors taken into account to prioritise the designated competent authorities' 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.

56. Since designated competent authorities should have already assessed the quality of risk management controls applied throughout casinos, 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 the individual casinos.

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

- Casinos or designated competent authorities 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 casinos need not be afraid of regulatory sanctions where they have acted responsibly and implemented adequate internal systems and controls.
- Regulators' staff must be well-trained in the risk-based approach, both as applied by designated competent authorities and by casinos.

## **SECTION TWO: GUIDANCE FOR PUBLIC AUTHORITIES**

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

57. The application of a risk-based approach to countering money laundering and the financing of terrorism will allow competent authorities and casinos 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.

58. 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**

59. 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.

60. National risk assessments should be tailored to the circumstances of each country. For a variety of reasons, including the structure of competent authorities and the nature of DNFBPs, including casinos, 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. Competent authorities, in consultation with the private sector, should consider how best to achieve this while also taking into account any risk associated with providing information on vulnerabilities in their financial and non-financial systems to money launderers, terrorist financiers, and other criminals.

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

61. 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.

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

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

### **Principle Three: Design of a supervisory framework to support the application of the risk-based approach**

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

65. Where appropriate, designated competent authorities should seek to adopt a risk-based approach to the supervision of casinos' 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 casinos, and the money laundering and terrorist financing risks to which these are exposed. Designated competent authorities will probably need to prioritise resources based on their overall assessment of where the risks in the casino's business are.

66. Designated competent authorities 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 wider duties. Where there is more than one competent authority overseeing casinos within a country, it is important that the authorities work co-operatively to avoid overlap or repetition.

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

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

### **Principle Four: Identifying the main actors and ensuring consistency**

69. 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, and some relevant authorities could operate at a state or provincial level. 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 casinos about how to implement a risk-based approach to AML/CFT.

70. 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.
- Internal revenue/tax services.
- Designated competent authorities.
- The private sector – This might include casinos, national and international trade bodies and associations, etc.
- The public – Arrangements designed to counter money laundering and terrorist financing are ultimately designed to protect the law-abiding public. However these arrangements may also act to place burdens on customers of casinos' businesses.
- Others – Those who are in a position to contribute to the conceptual basis underpinning the risk-based approach, such stakeholders may include academia and the media.

71. 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.

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

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

## **Principle Five: Information exchange between the public and private sector**

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

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

75. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. Financial Intelligence Units (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.

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

- Assessments of country risk.
- Typologies or assessments of how money launderers and terrorists have abused the DNFBPs, especially casinos.
- 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 casinos.
- Countries, persons or organisations whose assets or transactions should be frozen.

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

## Chapter Two: Implementation of the Risk-Based Approach

### *Assessment of Risk to Inform National Priorities:*

78. 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".

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

80. A national risk assessment should be tailored to the circumstances of the individual country, both in how it is executed and its conclusions, though countries should be mindful that money laundering and terrorist financing can often have an international dimension, and that such information may also add value to the national risk assessment. Factors that may influence the risk of money laundering and terrorist financing in a country could include the following:

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

81. 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 competent authority's view be made public? These are all questions for the competent authority to consider.

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

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

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

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

## **Regulatory Supervision – General Principles**

### Defining the acceptable level of risk

86. 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.

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

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

88. However, this does not exclude the need to implement basic minimum requirements. For instance, FATF Recommendation 5 (that applies to casinos through the incorporation of R.5 into R.12) states that “where [the casino] is unable to comply with (CDD requirements), it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transaction report in relation to the customer.” So the level of risk should strike an appropriate balance between the extremes of not accepting customers, and conducting business with unacceptable or unmitigated risk.

89. Where casinos are allowed to implement a risk-based approach, competent authorities expect casinos to put in place effective policies, programmes, procedures and systems to mitigate the risk and acknowledge that even with effective systems not every suspect transaction will necessarily be detected. They should also ensure that those policies, programmes, procedures and systems are applied effectively to prevent casinos 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’ occupations, type of account and account activities, types of products and services used, rated play etc. This is why developing an accurate customer profile is important in managing a risk-based system. Moreover, procedures and controls are frequently based on previous typologies cases, but criminals will adapt their techniques, which may quickly limit the utility of such typologies.

90. 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 will expect casinos 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 Casinos on Implementing a Risk-Based Approach.”

#### Proportionate Supervisory Actions to Support the Risk-Based Approach

91. Designated competent authorities 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. Authorities’ AML/CFT examinations should use risk-based audit techniques to identify high-risk casino activities to sample, and apply a risk-based analysis to measure casino strengths/weaknesses in this area.

92. In the course of their examinations, designated competent authorities should review a casino’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 casinos’ business and the adequacy of its mitigation measures. Where available, assessments carried out by or for casinos may be a useful source of information. The competent authority assessment of management’s ability and willingness to take necessary corrective action is also a critical determining factor. Designated competent authorities should use proportionate actions to ensure proper and timely correction of deficiencies, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or inadequate controls will result in the most severe supervisory response.

93. 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.

94. Designated competent authorities can and should use their knowledge of the risks associated with products, services, customers and geographic locations to help them evaluate casinos' money laundering and terrorist financing risk assessments, with the understanding, however, that they may possess information that has not been made available to casinos, and, therefore, casinos would not have been able to take such information into account when developing and implementing a risk-based approach. Designated competent authorities (and other relevant stakeholders) are encouraged to use that knowledge to issue guidelines to assist casinos in managing their risks. Where casinos are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by their competent authorities<sup>2</sup>. Guidance designed specifically for casinos is likely to be the most effective. An assessment of the risk-based approach will, for instance, help identify cases where casinos 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.

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

96. Under FATF Recommendation 24, designated competent authorities 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 must have the authority and willingness to apply fines and/or penalties in cases where substantial deficiencies exist. Often, action will take the form of a remedial program through the normal supervisory processes.

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

*a) Regulatory Transparency*

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

<sup>2</sup> FATF Recommendations 5 and 25, Methodology Essential Criteria 25.1 and 5.12.

99. 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 supervisory actions may be perceived as either disproportionate or unpredictable which may undermine even the most effective application of the risk-based approach by casinos.

*b) Staff Training of Designated Competent Authorities and Enforcement Staff*

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

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

102. The training should include instructing designated competent authorities 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 also should be satisfied that sufficient resources are in place to ensure the implementation of effective risk management.

103. To fulfil these responsibilities, training should enable designated competent authorities supervisory staff to adequately assess:

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

## SECTION THREE: GUIDANCE FOR CASINOS ON IMPLEMENTING THE RISK-BASED APPROACH

### Chapter One: Risk Categories

104. The factors described below affect customer risk and are not intended to be prescriptive or comprehensive. They will not apply universally to all casinos, and even when these factors are present there may be different risk outcomes for different casinos and operators depending upon a host of other factors. However, the factors are intended to act as a guide to help casinos conduct their own customer risk assessments, and to devise AML/CFT policies and procedures which accurately and proportionately reflect those assessments.

#### Country/Geographic risk

105. Some countries pose an inherently higher ML/TF risk than others. In addition to considering their own experiences, operators should take into account a variety of sources of information as identified by credible sources<sup>3</sup> identifying countries with risk factors that may result in a determination that a country poses a higher risk. Operators may wish to assess information available from non-governmental organisations which can provide a useful guide to perceptions relating to corruption in the majority of countries.

106. Customers that are associated with higher risk countries, as a result of their citizenship, country of business, country of residence, etc. may require enhanced due diligence, depending upon their overall risk level taking into account all other relevant factors.

107. Internet casinos may wish to check customer location because of the additional risks arising from transnational operations.

#### Customer risk

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

<sup>3</sup> “Credible sources” refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

- Customers that are Politically Exposed Persons (PEPs)<sup>4</sup>.
- High spenders<sup>5</sup>. Given the variations among casinos, the level of spending considered to be relatively high for an individual customer will vary among operators, and even among casinos owned and managed by the same operator. Customers may become high spenders because of their cumulative spending over a period of time (*e.g.* customers with relatively high level of spending with casino accountholder relationships). Similarly, casual customers who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders.
- Most casinos will have formal or informal policies which centre upon customers whom they consider to be high spenders. These policies may relate to commercial risk, or to marketing information to identify high spending customers provided with complementary goods and services (*e.g.* refreshments, food, entertainment, merchandise, lodging, show tickets and tickets to special events, or transportation). Some casinos offer special facilities to high spending customers, *e.g.* the use of VIP rooms to gamble away from the general public areas of casinos. Casinos need to ensure that AML/CFT policies, procedures and internal controls are applied consistently to customers in VIP rooms (particularly for casino due diligence, recordkeeping, suspicious activity reporting, and where required, currency transaction reporting).
- Disproportionate spenders. Casinos should devise policies relative to obtaining information about customers' financial resources, when feasible and available, to determine if customers fall into this category. These policies could be based on regulatory requirements or a risk-based decision on the part of the operator. One issue to consider is if and how casinos can gain an understanding of their customers' sources of income or wealth. This information could provide some insight as to the likely level of disposable assets which customers have available to gamble, (though this may only be feasible in practice when a customer makes a credit application). For example, the level of available assets is important in situations in which customers gamble on "credit". In addition, casinos should be alert to customers engaged in high value gambling that is inconsistent with a casino's information about customers' known levels or sources of assets (*e.g.* a customer's bank account) and/or income, or understanding of customers' occupations evidenced in casino credit account records (*i.e.* credit application), as well as any other information on file including established play at other casinos. If and when this information is obtained it may assist in assessing whether a customer's level of gambling is commensurate to her/his assets or level of legitimate income. For example, it may be advisable to scrutinise a customer with a relatively modest assets or income, who becomes a high spending customer.
- Casual customers. While casual customers can pose a heightened money laundering risk in some situations, it may be difficult to identify their associated spending patterns. This

<sup>4</sup> The FATF defines PEPs as follows: "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".

<sup>5</sup> Casinos should take into account the relative value of the monies in the country where the customer obtained their wealth. Land-based casinos should also take into account the relative value in the country where the customer is spending their money.

category would include tourists, although not all passing tourist trade will fall within this definition. Land-based casinos may host tourists on organised gambling tours (known as junkets), which are discussed below. However, even regular customers may pose a risk, particularly if their spending pattern changes, *e.g.* it dramatically increases or their rated play does not fit their playing profile *e.g.* minimal play.

- Improper use of third parties. Criminals may use third parties, or anonymous or identified agents to avoid CDD undertaken at a threshold. They may also be used to gamble, *e.g.* to break up large amount of cash. Third parties may be used to buy chips, or to gamble on behalf of others with minimal play (which may include early or high cash outs), or cash out/redeem chips for larger denomination currency, casino checks, etc.
- Junkets. Over-reliance on tour operators can pose a heightened money laundering risk especially in markets with resident populations that are too small to normally support casinos. In these instances, casinos can become overly dependent on junket representatives for business, a potential misuse of these services. In large markets, junket representatives are sources of premium players for casinos. In some countries, a casino may enter into a contractual agreement with a junket operator to rent a private room within a casino and in some situations, it is the junket operator, not the casino, which monitors player activity and issues and collects credit.
- Junket operators that provide premium players may exert commercial pressures on casinos in some countries, which may result in reducing scrutiny of individual spending patterns, or may try to unduly influence or exercise control over licensed casino operations. Further, junket organisers may engage in lending or the facilitation of lending to players outside casinos' knowledge. In addition, in some countries, junket organisers are allowed to 'pool' and therefore obscure the spending of individual customers, thus preventing casinos from making any assessment of customers' spending patterns.
- Also, licensed junket operators of record may be "fronting" for other junket operators in another country. The front operators supply players to a casino through a casino's licensed junket companies which may not qualify for licensure in the country where the players will be gambling. Such unlicensed sub-junket operators can act as unlicensed collectors of credit and may have ties to organized crime networks. Consequently, casinos would need to devise measures to identify and prevent junket organisers from engaging in informal arrangements that are inconsistent with risk-based AML/CTF policies, procedures and internal controls.
- Multiple casino player rating accounts. Some players will open up multiple player rating accounts with different names at the same casino and will provide different rating account numbers to casino raters at different times to hinder a casino's ability to track their gambling activities under the same customer name. Casinos will need to identify such accounts with similar players' names and the same physical descriptions (*e.g.* age, male or female, eye colour, hair colour, height, weight) to be able to monitor customers' aggregate gambling across their casino business. Casinos should implement policies, procedures, and systems to assist in the identification of customers opening multiple-player rating accounts for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid government reporting thresholds.
- Unknown Customers. Casinos in some countries have a problem with unknown customers that purchase large amounts of chips with currency at table games, engage in minimal or no play, and then redeem the chips for large denomination bills (*e.g.* EUR 500 or USD 100),

casino cheques or money/wire transfers. Casinos should implement procedures and systems to assist in the identification of unknown customers redeeming large amounts of chips for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.<sup>6</sup> This could extend to measures such as not cashing out such customers or cashing out by paying in small denomination bills, which are harder to hide or transport, as well as maintaining surveillance photographs and filing suspicious activity reports with physical descriptions.<sup>7</sup>

### Transaction risk

109. Casinos should consider operational aspects (*i.e.* products, services, games, and accounts/account activities) that can be used to facilitate money laundering and terrorist financing activities. In addition, land-based and Internet casinos have the following potential transaction risks:

- Proceeds of crime. However money is transferred to a casino, there is a risk that this money will have arisen from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking, theft from employer. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk.
- Cash. Customers may use a land-based casino to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport. Also, certain cash deposits by a customer, especially cash deposits which are considered relatively large either in relation to *i)* a particular casino's average receipts, or *ii)* what is known about a customer's financial status.

The majority of payments to Internet casinos are made directly from financial institution accounts. However, Internet casinos can operate as part of mixed gambling chains which also include betting shops and/or land-based casinos. It may be possible for customers to provide land-based outlets with cash which can then be credited to Internet casino accounts. Internet casinos should work closely with their land-based counterparts that initially receive the cash to ensure that CDD measures are applied, including verifying that the depositor is the account holder, and when appropriate, benefit is secured from the personal contact between land-based casino staff and customers.

- Transfers between customers. If Internet casinos wish to allow inter-account transfers between their customers they should devise careful policies and procedures which monitor the amount of the transfer(s). Internet casinos may also be aware of customers transferring money between themselves more informally without using their casino accounts, which should be taken into consideration in the casino operator's risk assessments.

Land-based casinos may also be aware of customers borrowing money from non-conventional sources, including other customers. Informal money lending can be illegal, and it can also offer criminals an opportunity to introduce proceeds of crime, usually cash, into the legitimate financial system through the casino. Again, this can pose a heightened risk.

- Loan Sharking (also known as usury). Casinos in some countries have a problem with this activity which is a crime that involves loaning money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under threat of violence. Loan sharks may be financed

<sup>6</sup> FATF Recommendation 12, Interpretative Notes for R. 5, 12 and 16, and Methodology Essential Criteria 12.1.

<sup>7</sup> FATF Recommendation 5 (that applies to casinos through the incorporation of R.5 and R.12).

and supported by organized crime networks. A loan shark usually preys on individuals who are struggling financially or, for some reason, are unwilling to seek credit from legal sources.

- Use of casino deposit accounts. Casinos will wish to encourage their customers to only use their deposit accounts for gambling purposes. Casinos need to consider what constitutes an abuse of such an account and should have policies, procedures, and internal controls, to prevent customers from using such accounts to deposit and withdraw without gambling or minimal play.
- Redemption of Chips, Tickets or Tokens for Currency. Casinos in some countries do not require that customers provide identification for the redemption of chips, tickets, or tokens unless it triggers government reporting thresholds. For a customer that has an established casino account number,<sup>8</sup> a casino, which is not required by governmental regulations to record such transactions at the cage, nonetheless should have policies, procedures, and internal controls to identify large redemptions<sup>9</sup> to such a customer that were paid with currency<sup>10</sup> (including any large cash outs without gambling for large denomination bills), or through issuance of a cheque.

110. There are a number of specific transaction issues which apply to Internet casinos (including “mobile casinos”):

- *Multiple casino accounts or casino wallets.*

An internet operator may own and control multiple web sites. Single web sites can also offer a range of different types of gambling. Operators will need to monitor customers' aggregate position across the whole of their casino business.

Customers may wish to separate the different types of gambling they are conducting with the same operator, or through the same web site, for legitimate reasons, *e.g.* to monitor their performance in different areas. Casinos should implement procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.

- *Changes to financial institution accounts.* Casino customers commonly use their accounts with financial institutions to gamble over the internet. Customers may hold a number of financial institution accounts, and they may wish to change which of these accounts they

<sup>8</sup> Types of casino accounts that a customer could have include deposit (*i.e.* safekeeping, front money or wagering), credit, check cashing, player rating or tracking, and slot club accounts.

<sup>9</sup> As part of a casino's risk-based prevention program, when a customer presents at a cage a large chip or token redemption, a cashier confirms it typically by a telephone call to a pit boss, floor person, card room supervisor, or other casino employee to determine if the chips were put at risk, or won at a table game as “verified winnings” or purchased at a table (*e.g.* when a customer is “walking with” chips at the end of table game play) to identify: *i*) potential counterfeit chips or tokens, *ii*) stolen chips or tokens, or *iii*) any temporary advance of chips to a customer (*i.e.* rim credit). Also, a cage cashier will query a casino's credit system for credit issuance (*i.e.* marker) and credit payment (*i.e.* marker redemption) activities for a customer with large chip or token redemptions.

<sup>10</sup> FATF's threshold of USD/EUR 3000 provides for identifying and verifying the identity of customers for example when cashing in casino chips or tokens and currency exchange. Also, the EU Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, Chapter I, Article 10, provides that “Member States shall require that all casino customers be identified and their identity verified if they . . . exchange gambling chips with a value of EUR 2000 or more.” Such identification and verification of customers with chip, ticket or token redemptions can be logically integrated with a casino's existing risk-based prevention program for AML/CFT purposes.

use in the casino. Casinos may wish to consider updating customer due diligence following such changes.

- *Identity fraud.* Details of financial institution accounts may be stolen and used on web sites. Stolen identities may also be successfully used to open financial institutions accounts, and such accounts may also be used on web sites. Internet Provider (IP) Number checks are useful in preventing criminals from opening multiple casino accounts using stolen identities, using the same computer. Casinos will be aware of these risks because of the 'charge back' system. Internet casinos also have a responsibility to protect their customers from having their identities stolen when using their web site, and will therefore wish to provide adequate security.
- *Pre paid cards.* Using cash to fund a pre-paid card poses similar risks as cash. Casinos cannot make the same level of cross reference checks on some types of pre paid cards as they are able to perform on financial institution accounts.
- *Electronic wallets (e- wallets).* Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. However, e-wallets which only accept money from financial institution accounts in the customer's name will not usually pose any greater or lesser money laundering risk than if funds are received directly from the financial institution. However Internet casinos should be aware that when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling. (See paragraph below regarding the related issue of casinos purposefully obscuring payments made to financial institution accounts held by customers).
- *Games involving multiple operators.* Poker games often take place on platforms (*i.e.* a central computer system that links electronic gambling devices for purposes of game selection, operation, monitoring, security, and auditing) shared by a number of different casino operators. The platform is likely to play a key role in monitoring the pattern and value of play for potential money laundering activities, *e.g.* chip dumping. The operator and the platform should have clear policies in respect to respective roles, alerts, enquiries, and subsequent actions, for AML/CFT.

#### Variables which affect risk

111. There are a range of variables which impact upon casinos risk levels. Some or all of these variables may impact upon the level of casinos risk, and upon the preventative measures necessary to effectively but proportionately tackle these risks.

- Whether a casino's business model centres upon either of the following options, or both of them:
  - (a) Attracting a large number of customers who gamble relatively small amounts of money, or
  - (b) Attracting a small number of customers who gamble relatively large amounts of money.
- Speed and volume of business.
- Types of financial services offered to customers.
- Types of payment, and payment methods, accepted from customers.

- Types of gambling offered *e.g.* table games, card games, electronic games (live or automated).
- The nature of the customers – whether they are regular/frequent customers or irregular/occasional customers.
- Whether the casino forms part of a bigger organisation owned by the same operator, for example:
  - (a) Whether the casino operator owns and manages other land-based and/or Internet casinos.
  - (b) Whether the casino, or its operator, offers different types of gambling, *e.g.* sports book, premium players.
  - (c) For Internet casinos, whether the operator has other web sites.
  - (d) For land-based casinos, whether the casino is stand-alone or integrated with other leisure facilities, *e.g.* a hotel.
- Whether the casino is wholly based in one country, or has a presence in multiple countries, *e.g.* whether a Internet operator's server is in a different country from other parts of it's business.
- Staffing numbers, turnover rate and experience levels.
- Type and effectiveness of existing supervision mechanisms (*e.g.* electronic and/or physical, loyalty clubs which monitor gaming activities).

112. Land-based casinos can also vary in the following ways:

- Size of premises.
- Customer profile.
  - (a) Whether the majority of customers are regular customers, including members. Or,
  - (b) Passing trade, including casual tourists or organised casino tours (known as junkets).
- Whether the casino is in a town or city centre location, or is more remote.
- Slot kiosk machines for ticket redemptions and maximum currency thresholds.
- “VIP” rooms or other facilities designed for high spending customers.

113. Another important variable is the level of general regulation of the casino, whether this occurs at a national or state/provincial level.<sup>11</sup> Casinos must be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CTF measures. An important aspect of such regulation is to ensure the honesty and integrity of casino staff. Special care should be taken to ensure that all staff members are aware of their casino's policy and procedures relating to assisting or facilitating customers to launder money.

114. Casinos may have commercial arrangements with some other organisations. Operators will want to ensure that their business partners, and their partners’ staff, are honest and credible, and this will also be helpful in terms of AML/CFT. Internet casino operators should be clear that ultimately they are responsible for any compliance failures, although for practical reasons they may need to task other organisations to ensure day to day compliance.

<sup>11</sup> At a minimum: *i*) casinos should be licensed; *ii*) competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino; and *iii*) competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

### Controls for Higher Risk Situations

115. Casinos should implement appropriate measures and controls to mitigate the potential money laundering risk of those situations that are determined to be higher risk as the result of individual business's risk-based approach. These measures and controls should include:

- Increased awareness and monitoring by casinos of higher risk customers and transactions across each business.
- Escalation for approval of an accountholder relationship with a higher risk customer.
- Increase levels of know your customer (KYC) or enhanced due diligence. For instance, enhanced customer due diligence checks must be undertaken on PEPs. These checks include obtaining information about the individual PEPs business or status, and their source of income in accordance with a country's legal and regulatory requirements. Senior management approval must also be obtained before a casino can do business with a PEP (see FATF requirements in Recommendation 6).

### **Chapter Two: Application of a Risk Based Approach**

116. Casinos adopt different strategies and approaches in the development of risk-based programs which are tailored to mitigate the money laundering and terrorism finance risks unique to their products, services, type of customers, and markets.<sup>12</sup> The strategies to manage and mitigate money laundering and terrorist financing risks in a casino should be designed to identify or prevent the activity from occurring through a combination of deterrence measures such as:

- Evaluation of customer and transaction risks.
- Management of customer accounts<sup>13</sup>.
- Appropriate CDD measures for customers (*e.g.* especially for deposit, credit and check cashing).
- Record keeping to assist criminal investigations.
- Detection, *e.g.* monitoring for and reporting of suspicious activity.

<sup>12</sup> Casinos operators who also offer non casino facilities may restrict AML/CFT measures to casino customers.

<sup>13</sup> Casinos should consider will constitute misuse of an account, and in what circumstances a customer's account will be closed.

## Customer Due Diligence

117. [Casinos should apply CDD to all customers when they engage in financial transactions in a casino at a particular financial threshold.<sup>14</sup> This threshold applies to either a single transaction, or to several transactions that appear to be linked.<sup>15</sup> Operators with multiple web sites should apply the threshold per customer not per website. A threshold approach requires particularly careful policies and procedures which ensure that the casino knows when customers reach the threshold. In these circumstances, the casino's procedures should include procedures to:

- Identify and verify the identity of each customer.
- Identify any beneficial owner (*i.e.* the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted<sup>16</sup>), and take reasonable risk-based measures to verify the identity of any beneficial owner. The measures that have to be taken to verify the identity of the beneficial owner will vary depending on the risk.
- Obtain appropriate additional information to understand the customer's circumstances and business.]

118. In many countries, CDD is performed upon entrance to the casino; those casinos should have mechanisms to be able to link that customer to specific financial transactions that the customer later engages in above the USD/EUR 3 000 threshold.

119. Staff monitoring in land-based casinos should cover, in particular:

- Customer staff ratio, particularly at busy periods.
- Communication within a casino.
- Whether or how customers will be advised of the relevant threshold, and about what checks will need to be undertaken if the threshold is reached, *e.g.* what documents customers will need to provide.

120. Land-based casinos should also consider how and when they will update CDD on regular customers.

121. Internet casinos may adopt specific methods of customer's identification. The FATF Recommendations recognise that non face to face business relationships or transactions can carry specific risks.<sup>17</sup> For that reason non face to face business requires alternative or additional compliance methods, especially in the area of CDD. These methods may rely upon new technologies, including the deposit and withdrawal methods offered on the website, and checks on the customer's IP address.

<sup>14</sup> The FATF threshold is USD/EUR 3 000.

<sup>15</sup> Examples of financial thresholds include the purchase or cashing in of casino chips, tickets or tokens, the opening of accounts, wire transfers, and currency exchange. Financial transactions do not refer to gambling transactions that involve only betting casino chips or tokens.

<sup>16</sup> This could include, for example, improper use of third parties as described above.

<sup>17</sup> Recommendation 8.

122. In the majority of cases Internet casinos do not meet their clients, except perhaps their high spenders. Internet casinos are therefore usually unable to form social relationships with them, or to form judgements as a result of those relationships. They are also unable to verify customer's physical appearance against photographic identification documents.

123. If casinos use software systems to assist with CDD the software should access a range of positive and negative checks. Although not available in all countries, public source data can be particularly valuable in identifying PEP's and individuals subject to various sanctions, as well as identifying associations with organised crime and/or terrorist financing activities. In addition, casinos may wish to do Internet searches in an effort to obtain additional information about a customer (see also paragraph 138 below).

124. If basic database checks are not sufficient, perhaps because of a raised risk level, Internet casinos can use a variety of other checks: *i*) traditional checks using customer's personal and official documents; *ii*) checks on customers' source of funds;<sup>18</sup> *iii*) using direct contact via telephone or email, using personal or electronic means.

### **Monitoring of Customers and Transactions**

125. Monitoring customers and their gambling is essential to ensure effective application of AML/CFT policies, procedures, internal controls and automated systems. Casinos are also likely to undertake monitoring for other reasons, including monitoring their commercial exposure and in relation to complementary benefits provided to customers, including discount of customer losses, as permitted by competent authorities.

126. Monitoring methodologies and processes need to take into account the resources of the casino. Land-based casinos that have surveillance departments use video recording media and maintain records that identify customer activity, should also include monitoring for potential suspicious transaction reporting. For example, a casino may use its surveillance system to assist it in monitoring customers who are conducting financial transactions which are unusual, suspicious, or potentially criminal in nature. Casinos may also consider barring customers because of false identification, inadequate identification; or suspicious transactions. Land-based casinos are able to observe their customers. This personal contact may assist with AML/CFT, provided staff are trained and remain alert.

127. The FATF Recommendations require casinos to keep records for five years. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence to criminal activity. Casinos are likely to keep sufficient records of transactions for other reasons, *e.g.* marketing and promotions.

128. With regard to Internet casinos, checks may be made on the location of the computer used when casino accounts are opened, or during gambling, including IP checks<sup>19</sup>. IP addresses provide information about the country where the computer being used is located.

129. It may be helpful to cross reference IP number information about jurisdiction with *i*) personal data provided by the player and the data provider by the Internet service provider; *ii*) the information the customer provides about their postal address and *iii*) if payment is made to the casino from a financial

<sup>18</sup> Casino operators can obtain full details of a customer's credit history from a credit reference agency with the written permission of the customer.

<sup>19</sup> Internet Service Providers can elaborate on IP addresses and traffic route.

institution account, the country where the financial institution account is held, which may be ascertainable from a BIN check.

130. Internet casinos are dependent upon IT systems. These IT systems should be adapted to ensure accurate monitoring of accounts and customers, and to ensure that adequate records are kept and retained. Decisions may need to be made about the necessary level of details of the transaction records which are retained. A risk based approach cannot solely rely upon IT, there must also be an element of human supervision and staff levels should be proportionate to risk levels.

### **Suspicious Activity Reporting**

131. In order to comply with legal or regulatory requirements casinos need to have systems in place which ensure that reports are made when required. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of suspicious activity under these circumstances is not applicable. A casino should allocate resources based on its risk assessment, focusing on those areas that present a greater vulnerability to money laundering and terrorist financing. Effective resource allocation will better assist the casino in identifying suspicious activity and filing reports. In preparing a STR, casinos are encouraged to use the most reliable customer records containing verified customer identification information, when available.

### **Training and Awareness**

132. Staff must be trained in accordance with their role and level/nature of responsibilities. Examples of the staff that will need to be trained are *i)* accounting staff, *ii)* finance department, *iii)* fraud management department, *iv)* information technology department, *v)* staff who deal with high spenders, *vi)* customer services staff, *vii)* compliance staff and *viii)* surveillance staff. For Internet casinos, such training should be addressed to information technology staff. Individuals who have responsibilities to monitor or approve transactions in connection with the gambling should receive more comprehensive training.

133. Applying a risk-based approach to the various methods available for training, however, gives each casino additional flexibility regarding the frequency, delivery mechanisms and focus of such training. A casino should review its own workforce and available resources and implement training programmes that provide appropriate AML/CFT information that is tailored to the appropriate staff responsibility and at the appropriate levels of detail and frequency.

## **Chapter Three: Internal controls**

134. When devising internal controls, casinos should consider their overall operation. Senior management should ensure that their ownership of the AML/CFT issue is visible at the Board or equivalent level and to all staff and business partners, including acknowledging their personal responsibility to ensure that there are adequate systems and controls in place. Senior management is in a position to influence the culture of their organisation, including encouraging a culture of compliance.

135. Casinos should develop and implement a framework of internal controls (*e.g.* policies, procedures and processes) for all operating divisions and departments reasonably designed to safeguard operations against money laundering and terrorist financing. AML/CFT internal controls should cover all related activities and programs such as suspicious activity reporting, currency transaction reporting (where required), customer identification, casino recordkeeping, records retention, and compliance. Internal controls should also include account opening and documentation procedures, and management information/monitoring systems adequate to detect and report suspicious activity in a timely manner to authorities. In addition, internal controls should mitigate the inherent risk of any high-risk account,

customer, product, or service as well as transactions to or from a high-risk country (*e.g.* sanctioned country, non-cooperative nation) that could be misused for money laundering or terrorist financing.

136. Casinos internal controls should be commensurate with: (a) complexity, organisation, and relative size of the business; (b) risks posed by the types of gambling and financial services offered as well as the volume of business; and (c) risks posed by the types of customers and geographical location. These controls may include:

- Measures for addressing higher risk customers and their transactions and accounts and ensuring adequate supervision and training of staff.
- Use of appropriate automated systems and programs.
- Establishment of a compliance function.
- Regular review and update of the risk assessment.

137. Casinos should conduct independent internal and/or external testing for AML/CFT programs with a scope and frequency commensurate with the risks of money laundering and terrorist financing they face, as well as the products and services provided, to determine if casinos procedures are comprehensive enough to detect suspicious activities. Casinos should take corrective actions once becoming aware of weakness and deficiencies in their AML/CFT risk-based programs, or any element thereof, that could or did result in failures to comply with governmental identification, reporting, recordkeeping, and record retention requirements.

138. Where available, and where permitted by domestic law, casinos may wish to:

- Subscribe to a national and/or an international reporting agency that provides on-line or telephonic searching of customer identification, which often can provide historical information on customers from other subscribing casinos concerning whether: (a) an individual applied for credit; and (b) a customer has any outstanding casino debts.
- Use public on-line database search engines that do not require a subscription.
- Subscribe to such data mining agencies that document criminal records, employers, occupations, asset locations, civil actions such as bankruptcies, liens and judgements, relatives and associates and other relevant information.
- Subscribe to organisations that provide searches from various business, government, legal, and news sources of documents to check on customers in question as well as provide customers' personal information (*e.g.* name, date of birth, address, place of birth) from their commercial databases.

## ANNEXES

### ANNEX 1 – SOURCES OF FURTHER INFORMATION

Various sources of information exist that may help governments, casinos 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 casinos may wish to draw upon. They provide additional sources of information, and further assistance might also be obtained from other information sources such as AML/CFT assessments.

#### A. Financial Action Task Force Documents

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

<http://www.fatf-gafi.org>

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

In determining the levels of risks associated with particular country or cross border activity casinos 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](http://www.imf.org/external/np/ofca/ofca.asp).
- Mutual evaluation reports issued by FATF Style Regional Bodies:
  1. Asia/Pacific Group on Money Laundering (APG)  
<http://www.apgml.org/documents/default.aspx?DocumentCategoryID=8>

2. Caribbean Financial Action Task Force (CFATF)

<http://www.cfatf.org/profiles/profiles.asp>

3. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)

<http://www.coe.int/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](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](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](http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm)
- UN Security Council Sanctions Committee – Country Status:  
<http://www.un.org/sc/committees/>

## ANNEX 2 – GLOSSARY OF TERMINOLOGY

### **Beneficial Owner**

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

### **Competent authorities**

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

### **Country**

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

### **Designated Non-Financial Businesses and Professions**

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

**FATF Recommendations**

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

**Identification data**

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

**Politically Exposed Persons (PEPS)**

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

## **ANNEX 3 – MEMBERS OF THE ELECTRONIC ADVISORY GROUP**

### **FATF and FSRB members and observers**

FATF: Argentina; Australia; Belgium; Canada; China; European Commission (EC); France; Hong Kong, China; Italy; Japan; Luxembourg; Netherlands; New Zealand; Portugal; Spain; South Africa; Switzerland; United Kingdom; United States.

FSRBs: APG - Chinese Taipei, Macao, China; EAG - Azerbaijan; GIABA - Nigeria; MONEYVAL - Romania; and OGBS.

### **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**

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.

### **Casino 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 (ABA), American College of Trust and Estate Council, Consejo General del Notariado (Spain), Council of the Notariats of the European Union, Council of Bars and Law Societies of Europe (CCBE), International Bar Association (IBA), Law Society of England & Wales, Law Society of Upper Canada.