Chapter One: Risk Categories 3.2 In order to implement a reasonable risk-based approach, financial institutions should identify the criteria to assess potential money laundering risks. Identification of the money laundering and terrorist financing risks, to the extent that such terrorist financing risk can be identified, of customers or categories of customers, and transactions will allow financial institutions to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making monitoring of customer transactions and on-going reviews a fundamental component of a reasonably designed risk-based approach. A financial institution may also have to adjust its risk assessment of a particular customer based upon information received from a competent authority. 3.3 Money laundering and terrorist financing risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling financial institutions to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer risk; and product/services risk. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, financial institutions will have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a financial institution’s discretion. 3.4 While there is no agreed upon set of risk categories, the examples provided herein are the most commonly identified risk categories. There is no one single methodology to apply to these risk categories, and the application of these risk categories is intended to provide a strategy for managing the potential risks. 23 Country/Geographic Risk 3.5 There is no universally agreed definition by either competent authorities or financial institutions that prescribes whether a particular country or geographic area (including the country within which the financial institution operates) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Factors that may result in a determination that a country poses a higher risk include: • Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (“UN”). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by a financial institution because of the standing of the issuer and the nature of the measures. • Countries identified by credible sources14 as lacking appropriate AML/CFT laws, regulations and other measures. • Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them. • Countries identified by credible sources as having significant levels of corruption, or other criminal activity. Customer Risk 3.6 Determining the potential money laundering or terrorist financing risks, to the extent that such terrorist financing risk can be identified, posed by a customer, or category of customers, is critical to the development of an overall risk framework. Based on its own criteria, a financial institution will determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include: • Customers conducting their business relationship or transactions in unusual circumstances, such as: o Significant and unexplained geographic distance between the institution and the location of the customer. o Frequent and unexplained movement of accounts to different institutions. And o Frequent and unexplained movement of funds between institutions in various geographic locations. • Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests. • Cash (and cash equivalent) intensive businesses including: 14 “Credible sources” refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk. 24 o Money services businesses (e.g. remittance houses, currency exchange houses, casas de cambio, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities). o Casinos, betting and other gambling related activities. And o Businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions. • Charities and other “not for profit” organisations which are not subject to monitoring or supervision (especially those operating on a “cross-border” basis)15. • "Gatekeepers" such as accountants, lawyers, or other professionals holding accounts at a financial institution, acting on behalf of their clients, and where the financial institution places unreasonable reliance on the gatekeeper. • Use of intermediaries within the relationship who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised. • Customers that are Politically Exposed Persons (PEPs). Product/Service Risk 3.7 An overall risk assessment should also include determining the potential risks presented by products and services offered by a financial institution. Financial institutions should be mindful of the risk associated with new or innovative products or services not specifically being offered by financial institutions, but that make use of the institution’s services to deliver the product. Determining the risks of products and services should include a consideration of such factors as: • Services identified by competent authorities or other credible sources as being potentially higher risk, including, for example: o International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank) and pouch activities. And o International private banking services. • Services involving banknote and precious metal trading and delivery. • Services that inherently have provided more anonymity or can readily cross international borders, such as online banking, stored value cards, international wire transfers, private investment companies and trusts. Variables That May Impact Risk 3.8 A financial institution's risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include: 15 See Special Recommendation VIII. 25 • The purpose of an account or relationship may influence the assessed risk. Accounts opened primarily to facilitate traditional, low denominated consumer transactions may pose a lower risk than an account opened to facilitate large cash transactions from a previously unknown commercial entity. • The level of assets to be deposited by a particular customer or the size of transactions undertaken. Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow for a financial institution to treat the customer as lower risk. • The level of regulation or other oversight or governance regime to which a customer is subject. A customer that is a financial institution regulated in a country with a satisfactory AML regime poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation. Additionally, companies and their wholly owned subsidiaries that are publicly owned and traded on a recognized exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate, recognised regulatory scheme, and, therefore, generally pose less risk due to the type of business they conduct and the wider governance regime to which they are subject. Similarly, these entities may not be subject to as stringent account opening due diligence or transaction monitoring during the course of the relationship. • The regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering perspective. • The familiarity with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a financial institution’s own operations within the country. • The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk. Controls for Higher Risk Situations 3.9 Financial institutions should implement appropriate measures and controls to mitigate the potential money laundering risks of those customers that are determined to be higher risk as the result of the institution's risk-based approach. These measures and controls may include: • Increased awareness by the financial institution of higher risk customers and transactions within business lines across the institution. • Increased levels of know your customer (KYC) or enhanced due diligence. • Escalation for approval of the establishment of an account or relationship. • Increased monitoring of transactions. • Increased levels of ongoing controls and frequency of reviews of relationships. 26 • The same measures and controls may often address more than one of the risk criteria identified, and it is not necessarily expected that a financial institution establish specific controls targeting each and every risk criteria.

Chapter Two: Application of a Risk-Based Approach Customer Due Diligence/Know Your Customer 3.10 Customer Due Diligence/Know Your Customer is intended to enable a financial institution to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The financial institution’s procedures should include procedures to: (a) Identify and verify the identity of each customer on a timely basis. (b) Take reasonable risk based measures to identify and verify the identity of any beneficial owner. And (c) Obtain appropriate additional information to understand the customer’s circumstances and business, including the expected nature and level of transactions. 3.11 The starting point is for a financial institution to assess the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. Financial institutions will determine the due diligence requirements appropriate to each customer. This may include: • A standard level of due diligence, to be applied to all customers. • The standard level being reduced in recognized lower risk scenarios, such as: o Publicly listed companies subject to regulatory disclosure requirements. o Other financial institutions (domestic or foreign) subject to an AML/CFT regime consistent with the FATF Recommendations. o Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds. o Transactions involving de minimis amounts for particular types of transactions (e.g. small insurance premiums). • An increased level of due diligence in respect of those customers that are determined to be of higher risk. This may be the result of the customer’s business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as: o Correspondent banking relationships; and o PEPs. Monitoring of Customers and Transactions 3.12 The degree and nature of monitoring by a financial institution will depend on the size of the financial institution, the AML/CFT risks that the institution has, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, financial institutions and their regulatory supervisors must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the perceived risks associated 27 with the customer, the products or services being used by the customer and the location of the customer and the transactions. Monitoring methodologies and processes also need to take into account the resources of the financial institution. 3.13 The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each financial institution’s analysis of its major risks. Regulatory authorities should, therefore, be mindful of and give due weight to the determinations made by financial institutions, provided that these determinations are consistent with any legislative or regulatory requirements, and are reasonable and adequately documented. 3.14 Monitoring under a risk-based approach allows a financial institution to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine adequacy for the risk levels established. Financial institutions should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented. Suspicious Transaction Reporting 3.15 The reporting of suspicious transactions or activity is critical to a country’s ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. Countries’ reporting regimes are laid down in national law, requiring institutions to file reports when the threshold of suspicion is reached. 3.16 Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of suspicious activity under these circumstances is not applicable. 3.17 A risk-based approach is, however, appropriate for the purpose of identifying suspicious activity, for example, by directing additional resources at those areas a financial institution has identified as higher risk. As part of a risk-based approach, it is also likely that a financial institution will utilize information provided by competent authorities to inform its approach for identifying suspicious activity. A financial institution should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions. Training and Awareness 3.18 Recommendation 15 requires that financial institutions provide their employees with AML/CFT training, and it is important that financial institution employees receive appropriate and proportional training with regard to money laundering and terrorist financing. A financial institution’s commitment to having successful controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees with at least general information on AML/CFT laws, regulations and internal policies. 3.19 Applying a risk-based approach to the various methods available for training, however, gives each financial institution additional flexibility regarding the frequency, delivery mechanisms and focus of such training. A financial institution should review its own workforce and available resources and implement training programmes that provide appropriate AML/CFT information that is: 28 • Tailored to the appropriate staff responsibility (e.g. customer contact or operations). • At the appropriate level of detail (e.g. front-line personnel, complicated products or customer-managed products). • At a frequency related to the risk level of the business line involved. • Testing to assess knowledge commensurate with the detail of information provided.

Chapter Three: Internal Controls 3.20 In order for financial institutions to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the institutions. Senior management is ultimately responsible for ensuring that a financial institution maintains an effective internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and engagement in AML is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the financial institution's policies, procedures and processes designed to limit and control risks. 3.21 In addition to other compliance internal controls, the nature and extent of AML/CFT controls will depend upon a number of factors, including: • The nature, scale and complexity of a financial institution's business. • The diversity of a financial institution’s operations, including geographical diversity. • The financial institution’s customer, product and activity profile. • The distribution channels used. • The volume and size of the transactions. • The degree of risk associated with each area of the financial institution’s operation. • The extent to which the financial institution is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non face to face access. 3.22 The framework of internal controls should: • Provide increased focus on a financial institution's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals. • Provide for regular review of the risk assessment and management processes, taking into account the environment within which the financial institution operates and the activity in its market place. • Designate an individual or individuals at management level responsible for managing AML/CFT compliance. • Provide for an AML/CFT compliance function and review programme. • Ensure that adequate controls are in place before new products are offered. • Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed. 29 • Provide for programme continuity despite changes in management or employee composition or structure. • Focus on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations. • Implement risk-based customer due diligence policies, procedures and processes. • Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals. • Enable the timely identification of reportable transactions and ensure accurate filing of required reports. • Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the institution’s AML/CFT programme. • Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel. • Provide for appropriate training to be given to all relevant staff. • For groups, to the extent possible, there should be a common control framework. 3.23 Senior management will need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of the financial institution. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the financial institution’s AML/CFT compliance programme. The testing should be riskbased (focusing attention on higher-risk customers, products and services); should evaluate the adequacy of the financial institution’s overall AML/CFT programme; and the quality of risk management for the financial institution’s operations, departments and subsidiaries; include comprehensive procedures and testing; and cover all activities