Financial Action Task Force

Public Consultation on the Draft Risk-Based Approach Guidance for the Securities Sector

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-money laundering / Countering the financing of terrorism
CDD	Customer[1] due diligence
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
IOSCO	International Organisation of Securities Commissions
ML	Money laundering
MLRO	Money Laundering Risk Officer
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations

[1] The industry often uses the term "client" which has the same meaning as "customer" for the purposes of this document.

RISK-BASED APPROACH GUIDANCE FOR THE SECURITIES SECTOR

This Guidance should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1, 10, 13, 17, 19, 20 and 26 and their Interpretive Notes (INR.), and the Glossary

other relevant FATF Guidance documents, such as:

- the FATF Guidance for the Banking Sector
- the FATF Guidance on Correspondent Banking Services
- the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment
- the FATF Guidance on Politically Exposed Persons
- the FATF Guidance Private Sector Information sharing
- the FATF Guidance on the Risk-Based Approach for Effective Supervision and Enforcement

relevant FATF typology reports, such as:

- the FATF Report: Money Laundering and Terrorist Financing in the Securities Sector

1. INTRODUCTION AND KEY CONCEPTS

1.1. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[2]. This Guidance focuses on RBA for the securities sector[3], and includes an annex on suspicious activity indicators in relation to securities. It takes into account the experience gained by public authorities and the private sector over the years in applying a RBA. This guidance should be read in conjunction with the 2009 report on money laundering and terrorist financing ("ML/TF") in the securities sector, which outlines vulnerabilities in the sector.

[2] www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[3] Securities activities are activities or operations described in the FATF Glossary under "Financial institutions", in particular points 7, 8, 9, 10 and 11. [*To consider what in addition to 7 (which covers trading activity) should be* referenced].

2. The RBA guidance for the securities sector was drafted by a group of FATF members and representatives of the private sector, co-led by a representative of Royal Bank of Canada and the United States[4].

3. The FATF adopted this updated RBA Guidance for the securities sector at its XX Plenary.

1.2. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to:

- Outline the key principles involved in applying a risk-based approach to Anti Money Laundering /Countering the Financing of Terrorism ("AML/CFT") in the securities sector;
- Assist countries, competent authorities, providers of securities products and services ("securities providers") and intermediaries in the risk-based design and implementation of applicable AML/CFT measures by providing general guidelines and examples of current practice;
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and
- Support the development of a common understanding of what the risk-based approach to AML/CFT entails in the context of the securities sector.

1.3. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance is aimed at the following audience:

- Countries and their competent authorities, including AML/CFT supervisors of the securities sector, and Financial Intelligence Units (FIU);
- Practitioners in the securities sector (including securities providers and intermediaries, and external examiners for AML/CFT purposes).

6. The Guidance consists of three sections. Section I sets out the key elements of the risk-based approach and needs to be read in conjunction with Sections II and III, which provide specific guidance to securities providers and intermediaries (Section II), and on the effective implementation of a RBA to supervisors of the securities sector (Section III). The annexes provide examples of countries' supervisory practices and suspicious activity indicators in the securities sector.

7. This Guidance recognises that an effective RBA will build on, and reflect, a country's legal and regulatory approach, the nature, diversity and maturity of its securities sector and its risk profile. It sets out what countries should consider when designing and

[4] The FATF Project group was composed of representatives from FATF members [International Organisation of Securities Commissions (IOSCO), Ireland, Luxembourg; Singapore and the USA] and from the private sector [Association for Financial Markets in Europe (AFME), Pershing, Philip Capital, Royal Bank of Canada, and the Securities Industry and Financial Markets Association (SIFMA)].

implementing an RBA; but it does not override the purview of national competent authorities. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework.

8. This guidance paper is non-binding. It draws on the experiences of competent authorities as well as AML/CFT professionals in the private sector and may assist both competent authorities and the private sector to effectively implement some of the Recommendations.

1.4. SCOPE OF THE GUIDANCE: TERMINOLOGY, KEY CHARACTERISTICS AND BUSINESS MODELS

1.4.1. Terminology

9. This Guidance applies to the provision of securities products and services. However, given the commonality of issues between the securities and banking sectors, such as issues raised by pooled account structures, banks offering securities products and services should consider this Guidance in conjunction with the FATF Guidance for a Risk-Based Approach: The Banking Sector.

10. The term "securities" is broadly defined for the purpose of this guidance as including, for instance:

- Transferable securities, including equities and bonds or similar debt instruments;
- Money-market instruments;
- Investment funds, including units in collective investment undertakings;
- Options, futures, swaps, forward rate agreements and any other derivative contracts relating to securities, currencies, interest rates or yields or other derivatives instruments, financial indices or financial measures, which may be settled physically or in cash;
- Options, futures, swaps, forwards and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash;
- Derivative instruments for the transfer of credit risk;
- Financial contracts for differences; and
- Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic variables, freight rates, emission allowances or inflation rates or other official economic statistics that are settled in cash, as well as any other derivative contracts relating to assets, rights, obligations, indices and measures not otherwise mentioned in this section, which have the characteristics of other derivative financial instruments.

11. It is important to note that the above definition is not to be considered as rigid nor exhaustive, as differences exist in terms of legal and regulatory definitions across different jurisdictions and as the securities sector continues to evolve constantly with the introduction of new securities products and services.

12. In some countries, crypto-assets and the associated Initial Coin Offerings (ICOs) are recognised as securities (and so subject to AML/CFT regimes); whereas other

countries have banned them. Some countries are also evaluating the appropriate regulatory framework for these products and services.

1.4.2. Key characteristics of the Securities Sector

13. The FATF Report on Money Laundering and Terrorist Financing in the Securities Sector (October 2009) outlines the main ML/TF vulnerabilities in the securities sector. Some of the key characteristics of the securities sector for the purpose of this Guidance for a Risk-Based Approach are as follows:

- The varying roles that securities providers and other intermediaries may play in different transactions; for example, a securities provider may be both an investment fund manager and a depository bank (see also paras 17-29 below);
- Differences among jurisdictions in terms of defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;
- ML/TF risks stem mainly from types of securities products and services, customers, investors and payment methods used in the securities sector; noting that cash is generally not accepted by securities providers in many jurisdictions;
- Global reach of the securities sector and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;
- Ability to transact in securities products via an intermediary which may provide a relative degree of anonymity;
- High liquidity of some securities products, which often enables their easy conversion to cash;
- Complex products that may be offered before they are regulated (or not regulated at all), before they are rated for ML/TF risks (e.g. the crypto-assets mentioned above), or both;
- Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents;
- An often highly competitive and sometimes incentive-driven environment, which may lead to a higher appetite for risk, or failure to adhere to internal controls;
- Pricing volatility of some products, particularly low priced securities;
- Transactions executed both on registered securities exchanges and elsewhere, such as over the counter transactions (where parties trade bilaterally), and reliance on alternative trading platforms, electronic communication networks and internet-based trading;
- Opportunity to use transactions in securities for generating illicit income within the sector, for example, market abuse or fraud.
- Challenges in pricing some securities products due to their bespoke nature or complexity.

14. Market abuse is a general term used to describe a wide range of types of unlawful behaviour in the financial markets including, without limitation, market manipulation, wash trading, insider trading, misappropriation, layering, unauthorized pooling, spoofing,

front running and the like. Chapter 4 of the FATF Typology Report on Money Laundering and Terrorist Financing in the Securities Sector (October 2009) provides additional information in relation to predicate offences for money laundering linked to securities.

15. Market abuse risk is relevant in the AML/CFT context for two principal reasons. Firstly, some forms of market abuse may constitute predicate offences for money laundering under applicable national laws. Secondly, certain controls which financial institutions may be required to implement to comply with market abuse laws, in particular the surveillance of trading activity may also be of utility in monitoring for suspicious activity for AML/CFT purposes.

16. This Guidance does not, however, purport to describe controls that financial institutions may be required to implement to prevent or detect market abuse. Further, whilst applicable laws may require financial institutions to report suspicions of market abuse to various authorities, references in this Guidance to report suspicious transactions are intended to relate to reporting suspicions of ML/TF (including market abuse, where appropriate) pursuant to Recommendation 20.

1.4.3. Securities Providers (services and activities)

17. For the purpose of this Guidance, securities provider means any natural or legal person who is, or is required to be, licensed or registered by a competent authority to provide securities products and services as a business. Securities providers range from those that largely interact with retail investors, such as retail stockbrokers, wealth managers and financial advisors, to those serving a largely institutional market like clearing houses, prime brokers and depository banks. This is not an exhaustive list of all securities providers, and in some instances securities provider may assume more than one of the above roles.

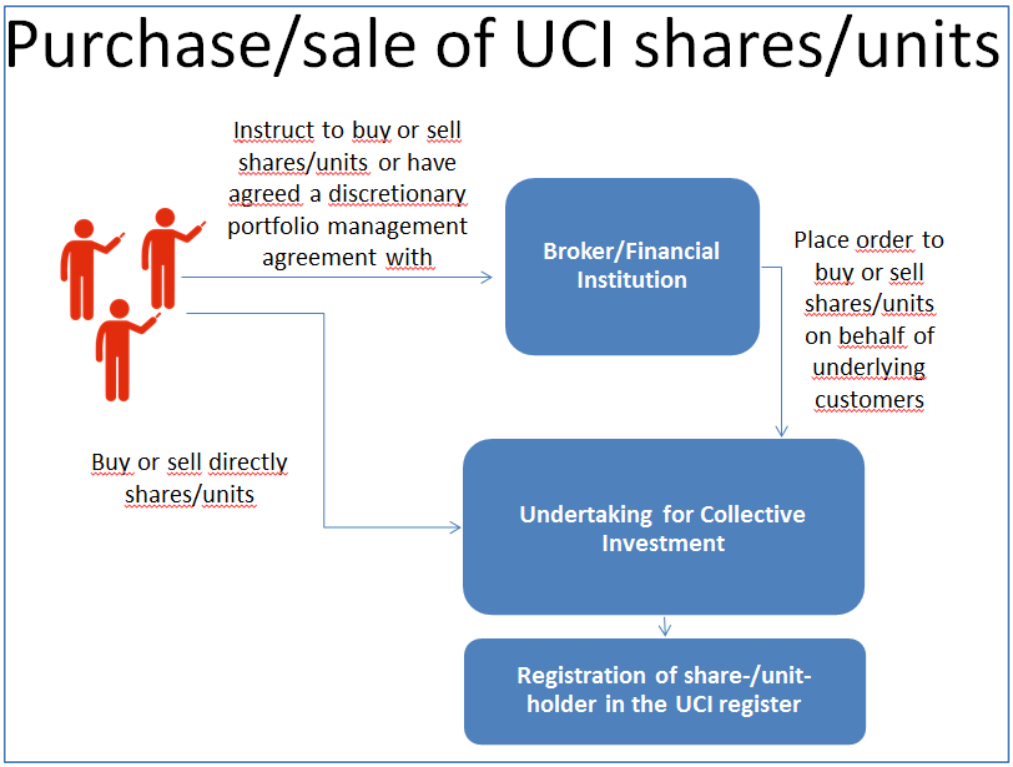
18. Securities providers offer various types of services, including buying and selling of securities, capital market research and advisory services, investment advice, individual and collective portfolio management, investment funds distribution, order execution services (trading in transferable securities), underwriting activity for issuers, private placements and other prospectus-exempt products, custody of client assets, lending money (providing margin) to clients and transfers of client cash (e.g. wire transfers) or securities, investment banking, mergers and acquisitions services, and syndicate and secondary market financing. Each of these activities and services may present different ML/TF risks depending on factors like the customer type, source and use of funds, customer business sector and geography. Securities providers typically specialise along retail, institutional and wholesale lines. Regardless of the role, the securities provider must continually tailor its own risk-based approach to assessing and managing ML/TF risk.

19. The risk-based approach to due diligence by securities providers can vary depending on a number of factors, such as securities product involved in a transaction, custodial relationships, contractual obligations, the customer, and applicable AML/CFT regulatory requirements, including customer identification requirements.

20. The CDD measures an investment fund should take will depend on how the customer or the investor (where the investor is not the customer) invests in the the fund. An investment fund, including undertakings for collective investment (UCIs) or pooled investment vehicles are undertakings established as limited companies, limited

partnerships or by contract that generally pool money from a number of third party investors and invest it in assets such as securities (e.g. stocks, bonds, and sometimes other mutual funds) or other assets (e.g. real estate, private equity and commodities). The combined investment holdings of the investment fund are known as its investment portfolio. Investors may buy and sell shares or units in investment fund. Each share/unit represents an investor's part ownership in the fund and the income it generates. Investors may buy and sell investment fund units directly from the fund itself or indirectly through an intermediary, such as a broker or financial institution. Depending on how the investment fund is sold and with whom the business relationship is established, the investment fund may be required to treat an investor as its customer or may be required to treat an intermediary as its customer. Where an intermediary is treated as the investment fund's customer, the investment fund may not have visibility on the intermediary's underlying customers. This includes not having comprehensive identification nor transaction-related information on the customers of the intermediary in cases such as, for example, where the intermediary nets all of its customers' orders and submits a single net order to the investment fund each day. When the intermediary is treated as the investment fund's customer and the intermediary's name is recorded in the investment fund's share/unit register, the arrangement is often referred to as an "omnibus" account. See illustration below, which demonstrates in simple terms one of the many distribution arrangements for investment funds(refer to Section 7.1.3).

Diagram 1- Illustration of ways in which shares/units in UCI shares/units are distributed



21. Another type of securities provider is an investment advisor, which can be either an individual or a firm that gives advice about securities to its customers. They typically provide advice on equities, bonds and funds to inform the customers of the types of investments available. These providers are likely to have direct interaction with their

customers, which may include individuals, institutions, trusts, or pooled investment vehicles.

22. A broker is a person or company that is in the business of buying and selling securities—stocks, bonds, mutual funds, and other investment products. A broker may have customers that are individuals, or other legal entities (including financial institutions, corporate entities, partnerships and trusts). Brokers vary widely in the types of services and products they offer to their customers.

23. Retail brokers fall generally into two categories—full-service and discount brokerage firms. Full-service firms often make investment recommendations and may have greater insight into their customers' investment goals, tolerance for risk and other data points. In contrast, discount or execution-only brokers often do not make recommendations and so may have more limited information about their customers. In either case, brokers will have visibility into their customer's transaction activity, whether acting on behalf of themselves or a third party. Where the broker's customer is, for example, another financial institution that introduces transactions on behalf of its own underlying customers—depending on the product introduced, in these arrangements visibility into the underlying customers can be limited.

24. While brokers serve customers who are interested in investing for retirement, saving for educational expenses and other common financial goals, brokers also provide services to other institutions, such as pension plans, hedge funds, banks and other brokers. One common arrangement where a broker provides services to another broker is an introducing/clearing arrangement. In that relationship, an "introducing broker" has the primary relationship with the underlying customer, and will take customer's orders for securities transactions. The introducing broker, in turn, passes along its customers' orders to a "clearing broker" for execution and clearing. The "clearing broker" may have little or no information about the introducing broker's underlying customers, although the clearing broker has visibility into and has an obligation to surveil any underlying customer transactions introduced to it.

25. Institutional brokers generally perform risk based due diligence (and enhanced due diligence, as applicable), on their legal entity customers. They are generally less focused on the investment goals and suitability of their customers as compared with retail brokers. Rather, an institutional broker's trading for a customer is often triggered based on the impact of varying market conditions. Underlying customer transparency and due diligence obligations depend on whether the relationship is execution, custody based and/or whether there is credit exposure to the underlying customer. For example, in a derivatives transaction, although the institutional broker may be dealing directly with an intermediary (e.g., an advisor) acting on behalf of its own underlying customer, the institutional broker will perform appropriate and necessary levels of due diligence on the underlying customer(s) to identify and mitigate any potential ML or credit risks identified.

26. Another type of securities provider is a custodial broker-dealer that is registered with a local supervisory authority, can be domiciled domestically or in a foreign jurisdiction, and can maintain custody of assets for its own customers (e.g. other broker-dealers, investment advisers, banks or other types of institutional clients) or their underlying customers. The underlying customers may be fully or partially disclosed to the custodial broker-dealer, while others may be non-transparent ("omnibus"). Regardless, customers' orders may be netted against each other by the broker-dealer's customer. Each type of direct customer of a custodial broker-dealer may present varying ML/TF risks that might require additional controls and other mitigation.

27. Securities providers known as clearing firms may provide record keeping, clearing, settlement and related functions associated with securities transactions and are unlikely to have visibility into the intent or suitability of any given transaction. While they may be in a position to identify specific securities transactions that are potentially suspicious (e.g., fraud, manipulative or deceptive trading practices), clearing firms generally do not have a direct relationship with the underlying customers in some jurisdictions. Therefore, in such cases, proper allocation of AML/CFT responsibilities with their intermediary who is responsible to conduct due diligence on its underlying customers, including retail or "introducing" broker-dealers, will maximize the AML/CFT efforts of each securities provider.

28. Prime brokers are another type of securities provider, who provides centralised clearing facilities for funds. They allow funds to borrow shares or money, and also act as record-keepers for other securities providers (e.g., investment advisers or investment managers) that are acting on behalf of pooled investment vehicle customers' transactions. In this context, the investment advisers or investment managers often establish customer account relationships by introducing pooled investment funds to multiple prime brokers. Securities providers may elect to mitigate potential risks in these scenarios through risk-based due diligence on associated "parties" (e.g., general partners of an investment adviser/investment manager).

29. The size and complexity of securities providers vary significantly and they use various business models. The complexity of the securities sector and the variety of securities provider roles highlight that where multiple securities providers are involved in a transaction, some securities providers may be in a better position than others to see various angles of that transaction. Thus, a securities provider should conduct an initial and ongoing risk assessment to understand and then mitigate any ML/TF risks identified.

1.4.4. Intermediaries

30. In the provision of their products and services, securities providers often interact with intermediaries, which may provide services on behalf of the securities provider, to a person or entity who is the customer of the intermediary, the securities provider, or both.

31. Services provided by these intermediaries could include performing certain aspects of customer due diligence (CDD) which are relied upon by a securities provider (reliance model- see paragraphs 101-103 for further description). Services may also include distribution services for selling securities products on behalf of a securities provider.

32. In other cases, securities providers may conduct transactions for certain other securities providers or intermediaries, which may be acting on behalf of their own customers All these different models and business practices may pose different ML/TF risks and require different approaches to mitigate such risks.

33. For example, under the reliance model, financial institutions are generally appointed by a securities provider to perform some aspects of CDD (identifying and verifying customers' identity, identifying and taking reasonable measures to verify beneficial owners, and understanding and obtaining information on the purpose and intended nature of the business relationship) under a formal agreement.

34. The distribution of securities products and services can involve multiple parties, such as distributors appointed by a securities provider, transfer agents, registrars and administrators, tied agents or proprietary distributors, and platform service providers.

35. The complexity of the securities sector and the variety of intermediary roles involved highlight that no one-size-fits-all AML/CFT approach should be applied. However, this variety and complexity underscores the importance to securities providers of understanding how their business arrangements raise ML/TF risks both directly (e.g., through transactions effected by customers) and more indirectly (e.g., risks associated with the underlying customers of the securities provider's customers, or risks associated with the possibility that an intermediary or other entity on which the securities provider relies to perform a task fails to do so).

1.5. INTERNATIONAL PROVISION OF SECURITIES PRODUCTS AND SERVICES

36. Some securities providers provide products and services across national borders through an intermediary or a network of intermediaries operating in another country. In instances where a securities provider operates in more than one country, the securities provider and competent authorities should verify that any ML/TF concerns are adequately addressed, in accordance with international standards and regulations in the jurisdictions in which they operate. This is without prejudice to supranational rules that would enable securities providers to supply services throughout the supranational jurisdictions subject to the applicable legal framework.

37. Cross-border provision of products and services (including through intermediaries or over the internet or otherwise) highlights the importance of international cooperation among the competent authorities of the relevant jurisdictions. Such international cooperation can be spontaneous or upon request depending upon the nature of the specific situation.

38. This Guidance provides more detail on the recommended actions for securities providers and competent authorities in sections 2 and 3 below.

SECTION I – THE FATF'S RISK-BASED APPROACH TO AML/CFT (RBA)

2. WHAT IS THE RBA?

39. The RBA to AML/CFT means that countries, competent authorities and financial institutions[5] are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

40. When assessing ML/TF risk[6], countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures[7]. For securities providers, this will require maintaining an understanding of the ML/TF risk faced by the sector as well as specific products and services, customer base, the capacity in which one's customers are operating (e.g., on their own behalf or on behalf of underlying customers, jurisdictions operated in, and the effectiveness of actual and potential risk controls that are or can be put in place). For supervisors, this will require maintaining an understanding of the ML/TF risks specific to the securities providers they supervise, and the degree to which AML/CFT measures can be expected to mitigate such risks. While institutions should strive to detect and prevent ML/TF, the RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate ML/TF risks, but it is still used for ML or TF purposes in isolated instances.

41. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low[8].

3. THE RATIONALE FOR A NEW APPROACH

42. In 2012, the FATF updated its Recommendations to strengthen global safeguards and to further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime.

43. One of the most important changes was the increased emphasis on the RBA for AML/CFT for all relevant public and private sector entities, especially in relation to

[5] Including both physical and natural persons, see definition of "Financial institutions" in the FATF Glossary.

[6] FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment, par. 10.

[7] FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment, par. 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

[8] Where the ML/TF risks have been assessed as low, INR. 1 allows countries not to apply some of the FATF Recommendations, while INR. 10 allows the application of Simplified Due Diligence measures to take into account the nature of the lower risk – see INR. 1 para 6, 11 and 12 and INR. 10 para 16 and 21.

preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework[9]. The RBA is an over-arching requirement applicable to all relevant FATF Recommendations.

44. According to the introduction to the FATF 40 Recommendations, the RBA allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, so they can focus their efforts in the most effective way.

45. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards[10].

4. APPLICATION OF THE RISK-BASED APPROACH

46. Recommendation 1 sets out the scope of the application of the RBA. It applies in relation to:

- Who and what should be subject to a country's AML/CFT regime: in addition to the sectors and activities already included in the scope of the FATF Recommendations [11], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF.
- How those subject to the AML/CFT regime should be supervised for compliance with this regime: AML/CFT supervisors should consider the securities provider's own risk assessment and mitigation, and acknowledge the degree of discretion allowed under the national RBA, while INR. 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision; and
- How those subject to the AML/CFT regime should comply: where the ML/TF risk associated with a situation is higher, competent authorities and securities providers have to take enhanced measures to mitigate the higher risk. This means that the controls implemented will be stronger, more numerous, wider in scope, more frequent, or a combination of these. Conversely, where the ML/TF risk is lower, standard AML/CFT measures may be reduced, which means that each of

[9] R. 1.

[10] The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance - *FATF Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems (2013).*

[11] See Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

the required measures has to be applied, but they may be applied more narrowly, less frequently, or in a reduced way [12].

5. CHALLENGES

47. Implementing an RBA can present a number of challenges:

5.1. Allocating responsibility under an RBA

48. An effective risk-based regime builds on, and reflects, a country's legal and regulatory approach, the nature, diversity and maturity of its financial sector, and its risk profile. Securities providers' identification and assessment of their own ML/TF risk should consider national risk assessments in line with Recommendation 1, and take account of the national legal and regulatory framework, including any areas of prescribed significant risk and any mitigation measures defined at legal or regulatory level. Where ML/TF risks are higher, securities providers should consider applying enhanced due diligence and monitoring, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree or frequency of ongoing monitoring)[13].

49. Securities providers may be granted flexibility in deciding on the most effective way to address other risks, including those identified in the national risk assessment or by the securities providers themselves. The securities providers' strategy to mitigate these risks has to take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which securities providers are able to decide how to mitigate risk, countries should consider, inter alia, their securities sector's ability to effectively identify and manage ML/TF risks as well as their supervisors' expertise and resources, which should be sufficient to adequately supervise how securities providers manage ML/TF risks and take measures to address any failure by securities providers to do so. Countries may also take into account evidence from competent authorities regarding the level of compliance in the securities sector, and the sector's approach to dealing with ML/TF risks. Countries whose financial services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that securities providers face challenges in effectively identifying and managing ML/TF risks and any flexibility allowed under the risk-based approach for simplified due diligence should therefore be limited[14].

50. Securities providers should not be exempted from AML/CFT supervision even where their capacity and compliance is good. However, the RBA should allow competent authorities to focus more supervisory resources on higher risk institutions and institutions providing higher risk products and services[15].

[12] R. 10; INR. 10, footnote 33.

[13] R. 1.

[14] This could be based on a combination of elements described in Section II, as well as objective criteria such as mutual evaluation reports, follow-up reports or FSAP reports.

[15] See FATF guidance on effective supervision and enforcement by AML-CFT supervisors of the financial sector and law enforcement.

5.1.1. Identifying ML/TF risk

51. Access to accurate, timely and objective information about ML/TF risks is a prerequisite for an effective RBA. INR. 1.3 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities, financial institutions and other interested parties. Information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk-based approach, and develop innovative techniques to combat ML/TF[16]. Enabling greater information sharing is a key element of collaboration whether it involves sharing across borders, between entities of the same financial group, between different financial groups or between private and public sector[17]. Jurisdictions should promote information sharing where possible, always seeking to ensure compatibility and coherence between local laws (including data protection laws) and AML/CFT laws. Where information is not readily available and adequate, it will be difficult for securities providers to correctly identify ML/TF risk and they may therefore fail to assess and mitigate it appropriately.

5.1.2. Assessing ML/TF risk

52. Assessing ML/TF risk means that countries, competent authorities and securities providers have to determine how the ML/TF threats identified will affect them. They should analyse the information obtained to understand the likelihood of these risks occurring, and the effect they could have, on the individual securities providers, the securities sector, and large scale financial institutions have on the national economy, if they did occur[18]. Risks identified through this process are often known as inherent risks, and risks which remain after the risk mitigation process are known as residual risks. During the course of a risk assessment, ML/TF risks may be classified as low, medium and high, with possible combinations between the different categories (medium-high; low-medium, etc.). These classifications are meant to assist in communicating ML/TF risks and to help prioritise them. Assessing ML/TF risk therefore goes beyond the mere collection of quantitative and qualitative information: it forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.

53. Assessing and understanding risks means that competent authorities and securities providers should have skilled and trusted personnel, recruited through fit and proper tests, where appropriate. This also requires them to be technically equipped to carry out this work, which should be commensurate with the complexity of the securities providers' operations.

5.1.3. Mitigating ML/TF risk

54. The FATF Recommendations require securities providers, countries and competent authorities when applying the RBA to decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. This implies that they should take enhanced measures to manage and mitigate situations in which the ML/TF

[16] See R. 18, R. 20, R. 21 and FATF Guidance on private sector information sharing.

[17] In the context of R.13, 16, 17, 18 and 26.

[18] Financial institutions are not necessarily required to perform probability calculations, which may not be meaningful given the unknown volumes of illicit transactions.

risk is higher; and that, correspondingly, in lower risk situations, simplified measures may be applied[19]:

- Countries looking to exempt certain institutions, sectors or activities from some of their AML/CFT obligations should assess the ML/TF risk associated with these financial institutions, sectors or activities and be able to demonstrate that the risk is low, and that the specific conditions required for one of the exemptions of INR. 1.6 are met. The comprehensiveness of the risk assessment will depend on the type of institution; sector or activity; products or services offered; and the geographic scope of the activities that stands to benefit from the exemption. The nature and complexity of the securities sector means that this exemption often will not apply.
- Securities providers looking to apply simplified measures should conduct an assessment of the risks connected to the category of customers or products targeted, establish the lower level of the risks involved, and define the extent and intensity of the required AML/CFT measures. Specific Recommendations set out in more detail how this general principle applies to particular requirements[20].

5.1.4. Developing a common understanding of the RBA

55. The effectiveness of an RBA depends on a common understanding by competent authorities and securities providers of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, securities providers must manage and mitigate the risks they identify. It is also important that competent authorities and supervisors in particular issue guidance to securities providers on how they expect them to meet their legal and regulatory AML/CFT obligations in a risk-sensitive way. Supporting ongoing and effective communication between competent authorities and securities providers is an essential prerequisite for the successful implementation of an RBA.

56. It is important that competent authorities acknowledge that in a risk-based regime, not all securities providers will adopt the same AML/CFT controls and that a single isolated incident of insignificant risk that has materialized may not necessarily invalidate the integrity of a securities provider's AML/CFT controls. On the other hand, securities providers should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls and that they must demonstrate to their competent authorities the effectiveness of the AML/CFT controls implemented, which should be commensurate with the risks identified.

57. Countries and competent authorities should take steps to effectively supervise all entities covered by AML/CFT requirements.

[19] Subject to the national legal framework providing for Simplified Due Diligence.

[20] For example, R. 10 on Customer Due Diligence and INR. 10.

SECTION II – GUIDANCE FOR SECURITIES PROVIDERS AND INTERMEDIARIES

58. This section should be read in conjunction with the *FATF Report on Money Laundering and Terrorist Financing in the Securities Sector* (October 2009), especially Chapter 3's summary of the main ML/TF vulnerabilities in the securities sector. The RBA consists of the identification of ML/TF risks and the definition and adoption of risk-sensitive measures that are commensurate with the ML/TF risks identified. In the case of securities providers, this applies to the types of products and services securities providers offer, the way they allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to manage and mitigate risk and detect and deter ML/TF. The RBA should also take into account intermediation networks.

6. RISK ASSESSMENT

59. Combating money laundering and terrorist financing is a global priority. The risk assessment should enable the securities provider to understand how, and to what extent, it is vulnerable to ML/TF. The risk assessment will also be developed as a result of regulatory requirements, guidance or expectations and will form the basis of a securities provider's RBA. It will often result in the categorisation of risks, including inherent and residual risks based on established controls and other mitigants which will help securities providers determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

60. The risk assessment should be properly documented, regularly updated and communicated to the relevant securities provider's senior management. A securities provider's risk assessment should be commensurate with the nature and complexity of the business, the type of products and services offered, the conditions of the proposed transactions, the distribution channels used and the customers' characteristics, among other things. This includes consideration of the following factors: i) the nature and size of the securities providers' business, including whether there are multiple subsidiaries, branches or intermediation networks offering a wide range and variety of financial products and services; ii) the risk profile of its customers, including whether its customer base is more diverse across different geographical locations; and iii)) other relevant risk factors unique to the securities provider's business model[21].

61. In conducting their risk assessments, securities providers should take into account quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate these risks[22]. This may include consideration of

[21] See R1 (c1.10 and c1.11)

[22] For example, in relation to terrorist financing, see the FATF Guidance on Emerging Terrorist Financing Risk (2015), and the countries that are in the FATF's International Cooperation Review Group (ICRG) process.

the risk and threat assessments, crime statistics, typologies, risk indicators, red flags, guidance and/or advisories issued by inter-governmental organisations, national competent authorities and FATF, and AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies. Furthermore, in identifying and assessing indicators of ML/TF risk to which it is exposed, a securities provider should consider a range of factors which may include:

- The nature, diversity and complexity of its business and target markets;
- The proportion of customers identified as high risk;
- The jurisdictions the securities provider is operating in or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as the prevalence of crime, corruption, financing of terrorism, as well as the general level and quality of the jurisdiction's prosecutorial and law enforcement efforts related to AML/CFT, the AML/CFT regulatory regime and controls, transparency of beneficial ownership, AML/CFT supervision by competent authorities;
- The distribution channels through which the securities provider distributes its products, including the extent to which the securities provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD or other AML obligations, the complexity of the transaction chain and the settlement systems used between operators in the payment chain, the use of technology and the extent to which intermediation networks are used;
- The internal and external (such as audits carried out by independent third parties, where applicable) control functions and regulatory findings; and
- The expected volume and size of its transactions, considering the usual activity of the securities provider and the profile of its customers[23].

62. Securities providers should review their assessments periodically and in any case, when their circumstances change or relevant new threats emerge. Securities providers should take into account input and perspectives from others within their organization, including those who interact with customers, compliance risk management, and internal audit departments (where relevant), in performing their periodic risk assessments.

63. ML/TF risks may be measured using various methods. The use of risk categories provides a strategy for managing potential risks by enabling securities providers to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer/investor risk; product/service risk; and intermediary risk.

64. The extent to which these risk categories are applicable and the weight they should carry (individually or in combination) in assessing the overall risk of potential ML/TF may vary from one institution to another, depending on their respective circumstances and risk management framework. Securities providers must have a comprehensive view of all risk factors relevant to their business, including how the

[23] INR. 1 and R.10.

certain risk factors may interplay and have an amplifying effect. For example, the risks inherent in a less well-developed securities sector could be greatly amplified by regional risks (if it is located, e.g., in an area where there is high incidence of drug trafficking). Consequently, securities providers will have to make their own determination as to the risk weights; at the same time, parameters set by law or regulation may limit a business's discretion.

65. As noted above, while there is no complete set of risk categories, the examples provided herein are the most commonly identified. There is no one single methodology to apply to these risk categories, and the following risk categories could be considered alone or in conjunction with other risk categories:

6.1. Country/Geographic Risk

66. There is no universally agreed upon definition or methodology for determining whether a particular country or geographic area (including the country/geographical area within which the securities provider or intermediary operates) represents a higher risk for ML/TF. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of higher risk include:

- Countries/areas identified by credible sources[24] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations organisation, or by national authorities as determined in each jurisdiction.
- Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.
- Countries considered to be uncooperative with respect to tax transparency, or refusing international cooperation due to their secrecy or offshore status.

67. Many governments and authorities carry out ML/TF risk assessments for their jurisdictions, and firms must take these into account when they are published, or have been communicated to the firms.

[24] "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF 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.

6.2. Customer/Investor Risk

68. Securities providers should determine whether a particular customer/investor[25] poses higher risk and analyse the potential effect of any mitigating factors on that assessment. Such categorisation may be due to customer's occupation, behaviour or activity. These factors considered individually, may not be an indication of higher risk in all cases. However, a combination of them may certainly warrant greater scrutiny. Categories of customers whose business or activities may indicate a higher risk include:

- Customer sanctioned by the relevant national competent authority for its non-compliance with the applicable AML/CFT regime and is not engaging in remediation to improve its compliance.
- Customer is a PEP or his/her family members or close associates are PEPs (including where a beneficial owner of a customer is a PEP) as covered under Recommendation 12.
- Customer resides in or whose primary source of income originates from high risk jurisdictions (regardless of whether that income originates from a cash-intensive business).
- Customer resides in countries considered to be uncooperative with respect to tax transparency, or refusing international cooperation due to their secrecy or offshore status.
- Customer acts on behalf of a third party and is either unwilling or unable to provide consistent information and complete documentation thereon.
- Customer has been mentioned in negative news reports.
- Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.).
- Customer is also a securities provider, acting as an intermediary or otherwise, but is either unregistered or registered in a jurisdiction with weak AML/CFT oversight.
- Customer is engaged in, or derives wealth or revenues from a potentially high risk cash intensive business.

6.3. Product/Service/Transactions Risk

69. A securities provider may offer a range of products/services to customers. An overall risk assessment should therefore include determining the potential risks presented by specific products and services offered by the securities provider. These products and services commonly involve executing transactions for a customer by processing an order to transact/trade and/or clear trades and handling the movement of funds or securities for the customer, and settling a customer's respective transactions and liabilities. The securities provider may also offer brokerage accounts as a custodian of a customer's assets. Transactional operations are either undertaken on a regulated exchange (e.g.,

[25] The use of the term "customer" covers "customer/investor" throughout the guidance.

NASDAQ) or other market or they may be conducted between parties directly. A securities provider should assess, using a risk-based approach, the extent to which the offering of its products and services present potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

70. Determining the risks of products and services offered to a customer may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:

- Products or services that may inherently favour anonymity or obscure information about underlying customer transactions (e.g., bearer share instruments, or the provision of omnibus account services).
- The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions.
- Products with unusual complexity and/or structure and with no obvious economic purpose (securities providers may offer this as an ancillary service or they may earn fees from the transactions), which may also make pricing the product difficult.
- Products or services which permit the unrestricted and/or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction.
- Use of new technologies or payment methods not used in the normal course of business by the securities provider.
- Products that have been particularly subject to fraud and market abuse, such as low-priced securities.
- The purchase of securities using physical cash.
- Offering bank-like products, such as check cashing and automated cash withdrawal cards.
- Securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from higher risk jurisdictions.
- The usage of brokerage accounts as long term depository accounts for funds.

71. Customer may request transactions that pose an inherently higher money laundering risk to the securities provider. This activity may be detected during transaction monitoring, although in many cases the customer's transactional activity may be apparent both during the point-of-sale interaction and back-end transaction monitoring. Some factors that may be considered as indicators of higher risk include:

- A request is made to transfer funds to a higher-risk jurisdiction/country/corridor without a reasonable business purpose provided.
- A transaction is requested to be executed, where the securities provider is made aware that the transaction will be cleared/settled through an unregulated entity.
- Transactions involve penny/microcap stocks.

6.4. Distribution Channel Risk

72. An overall risk assessment should include the risks associated with the different types of delivery channels to facilitate the delivery of securities products and services. Securities products and services are typically distributed directly to customers (including online) or through intermediaries.

73. A securities provider that distributes their products or services directly through online delivery channels should identify and assess the ML/TF risks that may arise in relation to distributing its products using this business model. In addition to the analysis of risks performed in advance of engaging of such an online business, the risk assessment process for online delivery risk should be performed when the securities provider develops new products and new business practices.

74. A securities provider should analyse the specific factors which arise from the use of intermediaries as a business model. The intermediary may be a part of the firm's distribution channel in its business model, or it may be a customer servicing itself and/or underlying customers (see Section 7.1.3). Intermediaries' involvement may vary with respect to the activity they undertake and their relationship with the securities providers. Some intermediaries may only introduce customers to the securities provider (the reliance model) whereas in other cases intermediaries may also use the products and services themselves or for their underlying customers (the omnibus model or cross border correspondent business relationships).

75. Regardless of the model, it is important for a securities provider to ensure that it understands who the intermediary is. The securities provider should perform a risk assessment on the intermediary prior to establishing a business relationship. It is also necessary for securities providers and intermediaries to establish clearly the respective responsibilities for compliance with applicable regulation. Assessing intermediary risk is more complex for securities providers with an international presence due to varying jurisdictional requirements, the potential risk of non-compliance by intermediaries with the applicable local AML/CFT regulations and the logistics of intermediary oversight. An intermediary risk analysis should include such factors as the following based on the extent that these are relevant to the securities providers' business model:

- Intermediaries suspected of criminal activities or association with criminal associates.
- Intermediaries located in a higher-risk jurisdiction/country or in a jurisdiction/country with a weak AML/CFT regime.
- Intermediaries serving high-risk customers.
- Intermediaries with a history of non-compliance with laws or regulation or that have been the subject of negative attention from credible media and/or law enforcement.
- Intermediaries that have failed to attend or complete AML/CFT training programmes requested by the securities providers.
- Intermediaries that have weak AML/CFT controls or operate sub-standard compliance programmes, i.e. programs that do not effectively manage compliance with internal policies and/or external regulation. or the quality of whose compliance programmes cannot be confirmed.

- Intermediaries whose underlying customer data collection or record keeping is inaccurate or inconsistent.

7. RISK MITIGATION

76. Having assessed ML/TF risks in their business, securities providers should then develop mitigating controls proportionate to the ML/TF risks identified and to the complexity, nature and size of the entity and activity. Consistent with the RBA, securities providers should allocate relatively more resources to mitigating their most significant risks.

7.1. Customer/investor Due Diligence and Securities and Related Money Transactions

77. Initial and ongoing due diligence will need to consider risks relating to:

- Customers acting on their own behalf;
- Intermediaries involved in the offer, sale, recommendation, or distribution of securities, acting on behalf of underlying customers (similar relationship to correspondent banking);
- Third parties on which a securities provider relies to discharge its AML/CFT obligations (reliance relationship).

7.1.1. Initial and Ongoing CDD

78. Securities providers should develop and implement policies and procedures to mitigate the ML/TF risks they have identified through their individual risk assessment. CDD processes should be designed to help securities providers understand who their customers are by requiring them to gather information on what they do and why they require their services. The initial stages of the CDD process should be designed to help securities providers assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

79. Based on a comprehensive view of the information obtained in the context of their application of CDD measures, securities providers should be able to prepare a customer risk profile. This will determine the level and type of ongoing monitoring and support the securities providers' decision whether to enter into, continue or terminate the business relationship. Risk profiles can apply at the individual customer level or, where groups of customers display similar characteristics (for example, customers with similar income range, or conducting similar types of securities transactions) the profiles can be applied to such groups.

80. Initial CDD consist of the following:

- Identifying the customer and, where applicable, the customer's beneficial owner;
- Verifying the customer's identity, and taking reasonable measures to verify the customer's beneficial owner on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; and

- Understanding the purpose and intended nature of the business relationship. In higher risk situations, obtaining further information, for ongoing monitoring of the business relationship and detection of potentially suspicious activity.

81. In addition, securities providers should take measures to comply with national and international sanctions legislation; sanction screening is mandatory and is not discretionary.

82. As a general rule, securities providers must apply CDD measures to all customers. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed in the Risk Assessment in the beginning of Section 2. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business relationship is lower. Securities providers therefore have to draw up, and periodically update, customer risk profiles, which serve to help securities providers apply the appropriate level of CDD. In some cases, information about the nature and purpose of a customer relationship may come from attributes inherent to the product.

83. In accordance with R10, where securities providers are unable to conduct the appropriate level of CDD, they should be required to not enter into the business relationship or terminate the business relationship.

7.1.2. Ongoing due diligence

84. A securities provider should conduct due diligence on its customers on an initial and ongoing/periodic basis. To this end, the securities provider should endeavour to be aware of material changes to the customer's legal form, beneficial ownership and/or nature of business. A securities provider should implement procedures to periodically review the customer relationship and CDD information. The risk-based periodic review process should be based on a formal cycle, and additional reviews should be performed based on "trigger-event" causes.

7.1.3. The Securities Provider's Customer

85. In addition to carrying out transactions and/or maintaining accounts for customers directly, securities providers may also deal with other securities providers and intermediaries who in turn have their own underlying customers. For illustration purposes, refer to paragraph 20, which provides an example of investment funds where the customer may be direct or indirect.

86. When determining the type and extent of CDD to apply, a securities provider should be clear whether the customer is acting on its own behalf or as an intermediary on behalf of its r underlying customers. Using a risk-based approach, including whether the intermediary is regulated for AML/CFT, the securities provider may obtain information about the intermediary's AML/CFT controls including the intermediary's risk assessment of its underlying customer base.

87. The intermediary is responsible for conducting CDD on its underlying customers and the securities provider should monitor the intermediary's transactions with a view to detecting any changes in the intermediary's risk profile or implementation of risk

mitigation measures (i.e. compliance with AML/CFT measures and applicable targeted financial sanctions), any unusual activity or transaction on the part of the intermediary, or any potential deviations from the agreed terms of the arrangements governing the relationship. Where such concerns are detected, the securities provider should follow up with the intermediary by making a request for information on any particular transaction(s), possibly leading to more information being requested on the underlying customers of the intermediary on a risk sensitive basis.

7.1.4. CDD considerations

88. CDD processes should be designed to meet the FATF standards and national legal requirements. The CDD process should help securities providers assess the ML/TF risk associated with a proposed business relationship. Securities providers should have policies, procedures, systems and controls which are up to date and effectively implemented to carry out CDD (a) when establishing business relations with that customer; (b) when carrying out occasional transactions above the applicable monetary threshold designated by the securities provider; (c) where they have suspicions of ML/TF regardless of any exemption or thresholds; and (d) where they have doubts about the veracity or adequacy of previously obtained identification data. Where a securities provider cannot obtain the information necessary to carry out CDD, Recommendation 10 provides that the securities provider not enter into a business relationship or carry out an occasional transaction, or terminate an already-existing business relationship, and consider making a suspicious transaction report in relation to the customer.

89. Depending on the complexity of their customer base and in accordance with the applicable regulations, securities providers should ensure that CDD processes allow them to establish customer risk profiles. Customer risk profiles should be informed by FATF standards, including those found in INR. 10, Recommendations/INR. 12-16 and by the risk and complexity of the securities products and services offered. This will determine the level and type of ongoing monitoring and support the securities provider's decision whether to enter into, continue or terminate the business relationship. Risk profiles can apply at the individual customer level or, customer group level, where a group of customers displays homogenous characteristics (e.g. customers conducting similar types of transactions or with the same economic activity). Securities providers should periodically update customer risk profiles[26], which serve to guide securities providers in applying the appropriate level of CDD.

90. When carrying out the initial CDD, securities providers should identify and take reasonable steps to verify the identity of the customer’s beneficial owner, where appropriate. This should be undertaken, on the basis of reliable and independent information, data or documentation, to at least the extent required by the applicable legal and regulatory framework (and subject to the application of simplified CDD measures in appropriate lower risk cases or enhanced CDD in higher risk cases). The CDD process also includes understanding the purpose and intended nature of the business relationship to form a basis for ongoing monitoring of the business relationship and with a view to facilitating the detection of potentially suspicious activity. When designing CDD procedures and conducting CDD on customers, securities providers should, where appropriate, consider the following issues:

[26] Based on the securities provider’s own risk assessment.

- **Purpose and intended nature of business:** A securities provider should ensure it has a clear understanding of expected activity to support ongoing transaction monitoring. Typically, the key consideration is being able to identify whether the customer's activity (e.g. transaction type, size or frequency) is in line with the securities provider's knowledge of the customer. Understanding the nature of the business relationship includes understanding any other parties involved within the relationship and the role the securities provider plays.
- **Beneficial ownership structures:** Where a customer appears to have a less transparent beneficial ownership or control structure, including the presence of corporate vehicles, nominees or private legal arrangements, a securities provider should ensure reasonable steps have been undertaken to verify the identity of beneficial owner(s), and to consider whether the opacity of the ownership structure of the identity of one or more beneficial owners is an indicator of elevated risk.
- **Source of wealth and funds:** Under the RBA, a securities provider should take reasonable measures to establish the source of wealth and source of funds of relevant parties, where necessary.
- **Considerations particular to intermediaries:** For customers that are intermediaries, securities providers should also consider whether:
    - the intermediary or the underlying customer is transacting with the securities provider on its own behalf or as an intermediary (see paragraphs 85-86 above);
    - the intermediary is incorporated in a jurisdiction assessed, by the securities provider, as being subject to equivalent AML/CFT standards;
    - the intermediary is subject to and supervised for compliance with satisfactory AML/CFT requirements;
    - the product or service is assessed, by the securities provider, as lower risk.

7.1.5. Enhanced CDD ("EDD") & Simplified CDD ("SDD")

91. The extent of CDD measures may be adjusted, to the extent permitted by applicable regulatory requirements, in line with the ML/TF risk. This means that the amount or type of information obtained, or the extent to which this information is verified, must be enhanced where the risk associated with the business relationship is higher. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. It may also be reduced where the risk associated with the business relationship is lower. Ongoing monitoring can also lead to a reassessment of the customer's risk profile, and should inform whether additional CDD or EDD is required.

92. It should, however, be noted that the derogation described in INR. 1.6(b), which permits countries to decide not to apply some FATF Recommendations to financial institutions conducting financial activity on an occasional or very limited basis, may not generally be appropriate for securities transactions, unless there is proven low risk of ML/TF. Similarly, it may not be appropriate to carry out SDD, rather than CDD on this basis alone. SDD measures are also not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

93. One example of when SDD measures may be appropriate is a pension product funded directly from a company's payroll; as such a product presents a lower ML/TF risk

than other products. Conversely, EDD measures must be required, for a PEP customer since such a customer presents heightened risks. Examples of both SDD and EDD measures are detailed below.

Box 1. Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR. 10)

Enhanced Due Diligence

- Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile
- Where appropriate, obtaining information about the intermediary's underlying customer base and its AML/CFT controls;
- Where appropriate, undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
- Obtaining additional customer information, such as the customer's reputation and background, before the establishment of the business relationship;
- Obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction
- Verifying the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime
- Evaluating the information provided with regard to the destination of funds and the reasons for the transaction
- Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship
- Requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer
- Increasing the frequency and intensity of transaction monitoring

Simplified Due Diligence

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer pieces of customer identification data
- Altering the type of verification carried out on customer's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established, without collecting additional information or carrying out additional measures related to understanding the nature and purpose
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction or account values rise above a defined monetary threshold). Reducing the frequency of customer identification updates in the case of a business relationship, if the securities

provider implements or is required to implement a periodic review process based on a formal cycle

- Reducing the degree and extent of on-going monitoring and scrutiny of transactions, for example based on a reasonable monetary threshold

7.1.6. Relationship similar to Correspondent Banking Relationship in case of Intermediaries

94. INR13 stipulates that for correspondent banking and other similar cross-border relationships, financial institutions should apply criteria (a) to (e) of R.13, in addition to performing normal customer due diligence measures.

95. A correspondent relationship is a relationship between the securities provider (correspondent), with an intermediary (respondent) , which is regulated and supervised by a supervisory authority, for securities transactions. In such cases, the customer of the respondent would not be considered as a customer of the correspondent, and the FATF Recommendations do not require the correspondent securities providers to conduct CDD on the customers of their respondent institutions.

96. Due diligence with regard to a correspondent relationship with a respondent generally takes place at two levels:

- Risk based due diligence on the respondent by using reliable, independent source documents, data or information (Rec. 10 (a)) and its beneficial owners, such that the securities provider is satisfied that it knows who the beneficial owner(s) of the respondent are. The securities provider should also verify the reputation of the respondent and the quality of its supervision; including whether and when it has been subject to targeted financial sanctions, a ML/TF investigation or regulatory action.
- Additional due diligence on the correspondent relationship with the respondent, as described below.

97. In accordance with Recommendation 13, correspondent securities providers in addition to performing customer due diligence on the respondent intermediaries, should also:

- Gather sufficient information about the respondent to understand the nature of the respondent's business and to determine from publicly available information the reputation of the respondent and the quality of its supervision;
- Assess the respondent's AML/CFT controls;
- Obtain approval from its senior management before setting up a correspondent relationship;
- Clearly understand the respective AML/CFT responsibilities of each institution.

98. In the case of a relationship similar to the correspondent banking, the correspondent generally does not have direct relationships with the customers of the respondent. In case the respondent allows its underlying customers to have direct access to its correspondent accounts (for example through a power of attorney or permitting the

underlying customer to place orders directly with the securities provider while settling them through the correspondent account), the securities provider must be satisfied that the respondent has conducted CDD on the customers having direct access to these accounts, and that it is able to provide relevant CDD information upon request.

99. Securities providers should also be prohibited from entering into, or continuing, a correspondent relationship with shell banks or shell securities providers. They should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks or securities providers.

7.1.7. Reliance on Intermediaries

100. In accordance with Recommendation 17 and where permitted by local legislation, a securities provider may reasonably rely on third parties to perform initial CDD. However, it may not rely on such parties to perform ongoing monitoring, ongoing due diligence and scrutiny of transactions. Specifically the securities provider should complete appropriate due diligence on the third party to determine whether reliance can be placed on the intermediary's AML/CFT risk and control framework and whether the intermediary is based in a country whose risk has been assessed by the securities provider (in accordance with R.17, § 1, c and d).

101. When reliance is appropriate, after consideration of the above, the ultimate responsibility for CDD remains with the securities provider – in other words, the provider can delegate the task but not the responsibility. In such situations, the securities provider should verify that the third party is conducting checks similar to or at a higher level than the securities provider's own internal standards. The securities provider should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in R.10, and also take adequate steps to confirm that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the third party upon request and without delay.

102. Securities providers should ensure that formal agreements which clearly set out the terms and conditions, including the roles and responsibilities of both the intermediary and the securities provider are in place.

7.1.8. Outsourcing

103. The reliance model above can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the securities provider, in accordance with its procedures, and is subject to the securities provider's overall control of the effective implementation of those procedures.

104. Under an outsourcing arrangement, a securities provider may also outsource ongoing monitoring and transaction monitoring. Securities providers should ensure that formal agreements which clearly set out the terms and conditions, including the roles and responsibilities of both the outsourced entity and the securities provider are in place.

105. The ultimate responsibility for CDD remains with the securities provider, again, it cannot delegate responsibility. In such a situation, the securities provider should ensure that checks are being conducted at a similar or higher level than the securities provider's own internal standards.

7.1.9. Electronic Wire Transfers requirements

106. R. 16 establish the requirements for countries with respect to wire transfers. R. 16 apply to both cross-border wire transfers and domestic wire transfers[27]. Securities providers who make wire transfers must include relevant originator and beneficiary information, where appropriate, on those wire transfers and ensure that the information remains with the wire transfer throughout the payment chain, as set out in the INR.16. It is important to note that countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer, and beneficiary information need not be carried out unless there is an ML/TF suspicion[28]. That is, for occasional cross-border wire transfers below USD/EUR 1 000, or the equivalent amount in local currency, the requirements of the INR.16 apply and the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number; however such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to the customer should be verified.

107. Securities providers that make wire transfers should adopt effective risk-based policies and procedures for determining when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information, as well as for defining and the appropriate follow-up actions[29]. In case of doubt, securities providers should clarify the responsibility for monitoring wire transfers between themselves and any other person involved in the wire transfer.

108. Where securities providers rely on payment service providers for fund transfers, depending on the arrangement, the responsibility for AML/CFT compliance with relevant electronic wire transfer requirements may likely be with the payment service provider.

7.2. Suspicious Transaction Monitoring and Reporting

7.2.1. Risk-based monitoring

109. Ongoing risk-based transaction monitoring is the scrutiny of transactions to determine whether they are consistent with the securities provider's information about the customer and the nature and purpose of the business relationship. This should include surveillance of securities transactions and money movements as well. Monitoring also involves identifying changes to the customer risk profile - for example, the customer's behaviour, use of products and the amount of money involved, and keeping this information up-to-date, which may trigger the application of enhanced CDD measures.

110. Transaction monitoring is an essential component of identifying transactions that are potentially suspicious. Transactions that do not fit the behaviour expected from a customer risk profile, that exhibit red flags of established money laundering typologies, or that deviate from the usual pattern of transactions, may be potentially suspicious. As part of their efforts to identify suspicious transactions, securities providers may also

[27] INR. 16 paragraph 3.

[28] INR. 16 paragraph 5.

[29] INR. 16 paragraph 18 and 22.

leverage surveillance frameworks implemented to detect predicate offences to money laundering, such as controls focussed on market abuse and insider dealing in securities.

111. A customer may transact across multiple jurisdictions in multiple financial firms which perform a variety of services in relation to securities transactions. Although information available may be limited, a securities provider may assess the following matters in order to determine the nature and extent of monitoring activity:

- The nature of the securities provider's customer base, including the country risk and whether customers are regulated or unregulated entities, and publicly or privately owned;
- The risk and complexity of products offered to customers;
- The volume and frequency of transactions processed by the securities provider; and
- The execution, clearing or settlement processes facilitated by the securities provider, including consideration as to whether payments to third parties are permitted.

112. Securities providers should take into account whether they have visibility into the underlying customer of an intermediary (whether related or unrelated to the provider) and whether they have the ability to fully ascertain all key information, whether required by applicable regulations or the securities provider's own risk assessment.

113. Transaction monitoring should be carried out on a continuous basis and may also be triggered by specific, unusual transactions. For example, a sudden spike in trading volumes can be an indicator of suspicious activity. However in the securities sector, market events, like corporate announcements, news or rumours on likely mergers or acquisitions, may also contribute to unusual trading patterns. Therefore, in conducting effective transaction monitoring, the securities provider should take into account such market events.

114. Securities providers should consider adjusting the extent and depth of monitoring based on their institutional risk assessments, customer risk profiles and the complexity of products offered. Enhanced monitoring should be required for higher risk situations. The adequacy of monitoring systems and the factors leading securities providers to adjust the level of monitoring should be reviewed regularly to verify that it is in line with the securities provider's overall AML/CFT risk programme.

115. Monitoring under a risk-based approach allows securities providers to create internal thresholds, based on a range of factors such as monetary amount or transaction number, to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. Securities providers should have the ability to flag unusual movements of funds or transactions for further analysis and should have systems that allow such funds or transactions are scrutinised in a timely manner and a determination to be made as to whether the funds movements or transactions are suspicious.

116. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent. Securities providers should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers.

117. Where automated systems are appropriate for use, securities providers should understand their operating rules, verify their integrity on a regular basis and check that they take account of the identified ML/TF risk typologies applicable for the securities sector.

118. Securities providers should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

7.2.2. Reporting Suspicious Activity

119. R.20 requires all financial institutions - including securities providers - that suspect, or have reasonable grounds to suspect, that funds are the proceeds of crime or related to terrorist financing, to report their suspicions promptly to the relevant FIU.

120. Transactions or movements of funds that are considered suspicious should be promptly reported to the FIU and in the manner specified by competent authorities. The processes securities providers put in place to escalate suspicions and ultimately report to the FIU should reflect this. While the policies and processes leading securities providers to form a suspicion can be applied on a risk-sensitive basis, a securities provider should report the activity once ML/TF suspicion has been formed.

121. Some jurisdictions require that suspicious market abuse (See Paras 14-16 above in relation to Market Abuse) be reported to a different authority (other than or in addition to FIU), generally the markets regulator. A securities provider should be aware of the specific reporting obligations required by the jurisdiction in which it is operating.

8. INTERNAL CONTROLS AND COMPLIANCE

8.1. Internal Controls and Governance

122. Adequate internal controls are critical components to an effective AML/CTF framework. Internal controls include appropriate governance arrangements that clearly allocate AML/CFT responsibilities, and controls to monitor the integrity of staff and intermediaries, implemented in accordance with the applicable local legislation. Securities providers should consider national or sectoral risk assessments and controls to validate that their policies and processes are effective tools for identifying, assessing, and monitoring ML/TF risks where they operate. It is appropriate for securities providers to modify their internal controls according to relevant changes in their size, operational complexity, or risk exposure. Accordingly, securities providers should maintain systems that are adequate and effective to manage and mitigate their risks. Where the risks are low, less sophisticated systems will suffice.

123. Securities providers which distribute their products or services through intermediaries, such as stockbrokers or funds platforms, should include these networks in their AML/CFT internal risk assessment processes.

124. The successful implementation and effective operation of an RBA to AML/CFT also depends on strong leadership by a securities provider's senior management team, which includes oversight of the development and implementation of the RBA across the securities provider.

125. Senior management should consider various ways to support AML/CFT initiatives, including:

- The fostering of a culture of compliance and promoting compliance as a core value of the securities provider by sending a clear message that the securities provider is committed to ensuring that:
  - ML/TF risks will be managed before entering into, or maintaining, business relationships or offering services that are associated with excessive ML/TF risks; and
  - Business relationships will not be established when the ML/TF risks cannot be mitigated and managed.
- Taking of responsibility together with the company board of directors (where applicable), taking responsibility for setting up robust risk management governance and controls mechanisms that:
  - Reflect the company's established risk policy;
  - Implement adequate internal communication processes appropriate for the actual or potential ML/TF risks faced by the securities provider. These mechanisms should link (where applicable) the board of directors, the top AML/CFT compliance officer, any relevant or specialised committee within the securities provider (e.g. the risks or ethics/compliance committee), the information technology division and each of the business areas;
  - Help to determine the measures needed to mitigate the ML/TF risks identified and the extent of residual risk the securities provider is prepared to accept; and
  - Include adequate resources for the securities provider's AML/CFT function.

126. This means that senior management should not only know about the ML/TF risks to which the securities provider is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- Understands the regulatory and supervisory requirements where the securities provider operates;
- Receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the securities provider is exposed through its activities and individual business relationships;
- Receives sufficient and objective information to understand whether the securities provider's AML/CFT controls are effective;
- Receives updates on government enforcement actions and other communications related to the AML/CFT obligations of securities providers and ML/TF risks; and
- Ensures that processes are in place to escalate important decisions that directly affect the ability of the securities provider to address and control risks.

127. Responsibility for the consistency and effectiveness of AML/CFT controls should be clearly allocated to an individual of sufficient seniority within the securities provider to signal the importance of ML/TF risk management and compliance, and of bringing

ML/TF issues to senior management's attention. This includes the appointment of a skilled compliance officer at the senior management level[30]. The group top AML/CFT officer should have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and across foreign branches and subsidiaries).

128. R.18 stipulates that countries should require financial institutions to have an independent audit function to test the AML/CFT programme with a view to establishing the effectiveness of an institution's AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. Senior management thus 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 securities provider. 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 securities provider's AML/CFT compliance programme. The testing should be risk-based, taking into account the risk profile of the securities provider; evaluate the adequacy of the securities provider's overall AML/CFT policies and programme and the quality of risk management for the securities provider's operations, departments and subsidiaries; include comprehensive procedures and testing; and cover all activities.

129. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance process or control failures or analysis of questions received from staff.

8.2. Compliance controls

130. A securities provider's internal control environment should be designed to achieve high standards of the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

131. The nature and extent of AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of a securities provider's business, the diversity of its operations, including geographical diversity, its customer base, and product and activity profile and the degree of risk associated with each area of its operations, e.g., the extent to which the securities provider is dealing directly with the customer or is dealing through intermediaries, third parties, or in a non-face-to-face setting without appropriate mitigating measures.

132. The framework of AML/CFT compliance function and internal controls should:

[30] INR. 18.

- Place priority on the securities provider's operations (products, services, customers and geographic locations) that are more vulnerable to abuse.
- Provide for regular review of the risk assessment and risk management processes, taking into account the environment within which the securities provider operates and the activity in those locations in which it operates.
- Provide for an AML/CFT compliance function and review programme which includes the testing of key components.
- Verify that adequate risk assessment and controls are in place before new products are offered.
- Regularly inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
- Provide for programme continuity despite changes in management or employee composition or structure.
- Focus on meeting all appropriate regulatory record keeping and reporting requirements and requirements for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enable the timely identification and filing of reportable transactions.
- Provide for adequate management and oversight of its intermediaries, including initial intermediary due diligence, AML/CFT training, and ongoing risk-based monitoring.
- Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the business's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Ensure that staff or firm performance is not the driver for taking disproportionate ML/TF risks.
- Provide for appropriate initial and refresher training to be given to all relevant staff.
- Provide for initial and refresher training for intermediaries, as applicable, at appropriate intervals.

8.3. Vetting and recruitment

133. Securities providers should conduct background checks on staff as part of the recruiting process to satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls, whether in the compliance or front-line functions.

134. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

8.4. Training and Awareness

135. The effective application of AML/CFT policies and procedures depends on the understanding of securities providers' staff on the relevant requirements and accompanying processes they are required to follow and the risks these processes are designed to mitigate. This training is designed to mitigate potential ML/TF risks occurring by, at or through a securities provider. It is therefore important that staff receive AML/CFT training, which should be:

- Relevant to the securities provider's ML/TF risks and business activities and up to date with the latest legal and regulatory obligations and internal controls;
- Obligatory for all appropriate staff;
- Tailored, where applicable, to particular lines of business within the securities provider, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks; this may be particularly important with regard to staff responsible for identifying fraud and market abuse, which may be reportable as a suspicious transaction;
- Effective, as measured, for example, by requiring staff to pass tests as part of the training or by monitoring levels of compliance with the securities provider's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
- Regular, relevant, and not a one-off exercise when staff are hired, in line with INR. 18, and;
- Complemented by AML/CFT information and updates that are disseminated to relevant staff, as appropriate.

136. Overall, the AML/CFT training should also seek to build a culture in which compliance is embedded in the activities and decisions by its staff.

SECTION III – GUIDANCE FOR SUPERVISORS

137. The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate to the ML/TF risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of a risk-based approach by securities providers.

9. THE RISK-BASED APPROACH TO SUPERVISION

138. R. 26 requires countries to subject securities providers to adequate AML/CFT regulation and supervision. INR. 26 requires supervisors to allocate supervisory resources to areas of higher ML/TF risk, based on supervisors' understanding of the ML/TF risks in their country, and to have on-site and off-site access to all information relevant to determining a securities provider's risk profile. There is a higher supervisory standard for the supervision of institutions subject to core principles.

Box 2. Recommendation 26: Regulation and Supervision of Financial Institutions

[…..] For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions (for intermediaries) should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. […..]

Additional sources of information

- Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis - The Risk-Based Supervision Guidelines published by the European Supervisory Authorities (April 2017).
- Principles on customer identification and beneficial ownership for the securities industry published by the IOSCO (May 2004).
- AML Guidance for collective investment schemes published by the IOSCO (October 2005).

9.1. Understanding ML/TF Risk

139. Supervisors should understand the ML/TF risks to which the securities sector is exposed[31], and the ML/TF risks associated with securities providers, both at an individual

[31] Consistent with IOSCO Core Principle (ICP) 6.

firm level and a financial group level, as well as the different securities sub-sectors in which they operate. Supervisors should draw on a variety of sources to identify and assess ML/TF risks, including information from stock exchanges and self-regulatory organizations

140. For sectoral risks, these are likely to include, but will not be limited to, the jurisdiction's national and sectoral risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback.

141. For individual securities providers, supervisors should take into account the level of inherent risk for that provider including the nature and complexity of its products and services, size and business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location and countries of operation. Supervisors should also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions, the history of the securities provider's compliance with regulations, STR reporting history (including quality, timing and volume of STRs submitted) and other open source information.

142. Some of this information should be obtained from the supervised entities (e.g. on the size, business model, location and nature of business etc.). Some of this information can also be obtained through prudential supervision or routine supervisory oversight of the sector. Other information, which may be relevant in the AML/CFT context, includes the fitness and propriety of the senior management and the adequacy of the compliance function[32]. In some jurisdictions, this may involve information-sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to two or more separate agencies.

143. Information from the securities provider's other stakeholders such as other supervisors, industry bodies, FIUs and law enforcement agencies may also be helpful in determining the extent to which a securities provider is able to effectively manage the ML/TF risk to which it is exposed.

144. Supervisors and other competent authorities should review their assessment of both the sector's and a specific securities provider's ML/TF risk profile periodically, and when a provider's circumstances change or relevant new threats emerge. These threats could include, for example, new products and delivery channels that pose ML/TF risks, or the absence of local regulations sufficiently to govern the new products and delivery channels.

145. Examples of different ways by which securities supervisors assess ML/TF risk in the securities sector and in individual securities providers can be found in Annex A.

9.2. Mitigating ML/TF Risk

146. The FATF Recommendations require supervisors to allocate more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual securities providers are exposed. It also means that where detailed supervision of all securities providers for AML/CFT purposes is not feasible,

[32] As specified in ICP 3.

supervisors should give priority to the areas posing higher risk, either in the individual securities provider or to securities providers operating in a particular sector.

147. Examples of ways in which supervisors can adjust their approach include:

a) **Performing additional enhanced checks, as appropriate, as part of their authorisation function:** supervisors can adjust the level of information they require when working to prevent criminals or their associates from holding a significant or controlling interest in a securities provider. For example, where the ML/TF risk associated with the applicant is considered low (e.g. due to ownership structure, nature of business and role in a securities transaction), the associated opportunities for ML/TF may also be limited and thus supervisors may decide to base their approval decisions on a review of relevant documentation. Where the associated ML/TF risk is considered high, supervisors may ask for additional information and set out more elaborate processes, including for example face-to-face interviews, criminal record and background checks, liaisons with other authorities, etc.

b) **Adjusting the type of AML/CFT supervision:** supervisors should always have both on-site and off-site access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can also determine the correct mix of on-site and off-site supervision. Off-site supervision alone may not be appropriate in higher risk situations.

c) **Adjusting the frequency and nature of ongoing AML/CFT supervision:** supervisors should adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge, e.g., as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from, for example, general supervision or a provider's inclusion in supervisory review areas (e.g. focused reviews of particular products or services or particular types of providers or customers, or particular areas of interest such as identification and verification of beneficial ownership by securities providers, distribution channels used etc.).

d) **Adjusting the intensity of AML/CFT supervision**: supervisors should decide on the appropriate scope or level of assessments in line with the risks identified[33], with the aim of assessing the adequacy of a securities provider's policies and procedures that are designed to prevent them from being abused[34]. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the provider's risk assessment, CDD, reporting and record keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT assessment in particular lines of business.

148. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and AML/CFT rules and guidance remain adequate. Whenever appropriate,

[33] BCP 10.

[34] In line with BCP 31.

these findings should also be communicated to the provider to enable them to enhance their RBA.

149. In line with R.26 and the application of the International Organisation of Securities Commissions (IOSCO) Core Principles relevant for AML/CFT[35], securities supervisors should consider the results of other prudential or financial supervision in their AML/CFT supervisory activities. Similarly, they should check that the broader prudential findings that drive the overall supervisory strategies of securities providers are informed by, and adequately address, the findings of the AML/CFT supervisory programme.

150. Under FATF R.27 and R.35, supervisors should have the power to impose adequate sanctions on securities providers and intermediaries when they fail to comply with AML/CFT requirements. Supervisors should use proportionate actions, which may include a range of supervisory interventions, including remedial/corrective actions to ensure proper and timely correction of identified deficiencies as well as punitive sanctions for more egregious non-compliance, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or significant failure in controls will result in a more severe supervisory response.

9.3. AML/CFT Supervision of Securities Providers in a Cross Border Context

151. For cross-border supervision purposes, supervisors of the home jurisdiction should have access to the customer, account and transaction information maintained by the financial institution in the host jurisdiction, to the extent permissible under the legal frameworks of both jurisdictions. This should include STR or STR-related information, where this is necessary to assess compliance with AML/CFT obligations and the robustness of risk management procedures. While host supervisors will be assessing compliance with local laws and obligations, home supervisors should have the ability to assess compliance with group-wide AML/CFT policies and procedures.

152. Lack of such access may inhibit the ability of the home supervisor to effectively assess group compliance, thereby affecting the effective implementation of FATF Recommendations. If the reasons for the denial of access prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisors should make it clear to the host supervisor that the financial institution may be subject to additional supervisory actions, such as enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host jurisdiction.

153. In adopting a RBA to supervision, countries and competent authorities may choose to consider allocating supervised entities which share similar characteristics and risk profiles into groupings for supervision purposes. Examples of characteristics and risk profiles could include the size of business, type of customers serviced, geographic areas of activities and delivery channels. The setting up of such groupings could allow competent authorities to take a comprehensive view of the securities sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual securities provider or intermediary. If the risk profile of a securities provider or

[35] IOSCO Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D.

intermediary within a grouping changes, the supervisor may wish to reassess the supervisory approach, which may include removing the securities provider or intermediary from the grouping.

10. SUPERVISION OF THE RISK BASED APPROACH

10.1. General Approach

154. Supervisors should encourage and monitor securities providers' adoption of an RBA that is in line with the FATF recommendations, and that is risk-appropriate given the provider's respective business models, size of operations, and operating environments.

155. Supervisors should note that under the RBA, particularly in the securities sector given the diversity in business models and domestic regulatory requirements, there may be valid reasons for differences in securities providers' controls. There is therefore no one-size-fits-all approach. In evaluating the adequacy of their RBA, supervisors should take into consideration the merits of these differences.

156. The securities sector is likely to be inter-connected with the rest of the financial system, in particular the banking system. Supervisors should get a good understanding of the effect of such interconnections on the ML/TF risk of the securities providers, and make appropriate adjustments where necessary to the supervisory RBA.

157. The task of supervising the implementation of the risk-based approach is a challenging one. To be effective, the following are some of the necessary preconditions:

- **Adequate understanding of ML/TF risk in the sector, subsector and individual firms.** Supervisors should adopt measures to acquire and maintain adequate and up to date knowledge of the ML/TF risks faced by the industry. They should, in particular, have a thorough understanding of the higher and lower risk lines of business. This understanding should help supervisors form a sound judgment about the proportionality and adequacy of AML/CFT controls.
- **Adequate resources and skillsets.** Supervisors should have adequate financial, human and technical resources to properly conduct the risk-based supervision approach. In assessing whether supervisors possess adequate resources, pertinent considerations include the size and complexity of the sector and the level of ML/TF risks faced by the sector.
- **Strong supervisory focus on effective implementation of controls by securities providers.** Basic compliance with the relevant laws and regulations is necessary but not sufficient. For the RBA to be effective, supervisors should also focus on assessing the quality of the securities providers' controls, whether the controls are effectively implemented, and whether the controls are able to effectively mitigate the ML/TF risks that they face. Supervisors need to clearly articulate and communicate their expectations, including the necessary rectification measures where there are shortfalls in providers' controls.

10.2. Training

158. Training is important for supervision staff to understand the securities sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a securities provider's ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of the securities provider's AML/CFT policies, procedures and internal controls in light of its risk assessment.

159. Training should allow supervisory staff to assess and form sound judgments about the quality of the securities provider's risk assessment and effectiveness of the securities provider's AML/CFT control. It should also aim at achieving consistency in the supervisory approach conducted at the national level, in the case of multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

160. Given the diversity and complexity within the securities sector (e.g. due to emergence of new business models and technologies), supervisory authorities should conduct continuous training programmes for supervisors, so that they can develop and maintain their proficiency. A training programme could include the following topics:

- General AML/CFT issues;
- Business models of various sub-segments of the securities sector (e.g. broker-dealers, fund managers) and the associated ML/TF risk issues;
- Interaction among the various sub-segments of the securities sector, and with other parts of the financial system (e.g. the banking system), as well as the impact on the scale and nature of ML/TF risks;
- International regulatory actions, such as economic sanctions;
- National and international supervisory cooperation mechanisms; and
- Other pertinent issues (e.g. implementation of common reporting standards, enhancing transparency of beneficial ownership, and the effect of financial technology developments on ML/TF risks).

10.3. Guidance

161. Supervisors should communicate their expectations of financial institutions' compliance with their legal and regulatory obligations. This could be done through a consultative process after engaging with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to securities providers should also discuss ML/TF risk within their sector and also outline ML/TF indicators (transactional and behavioural) in order to help them identify suspicious transactions. Supervisors should also consider issuing guidance to financial institutions on how to comply with their legal and regulatory AML/CFT obligations in a way that fosters financial inclusion.

162. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the industry, which may cover operational issues, and be more detailed and explanatory in nature. Securities providers should note,

however, that the private sector guidance they take into consideration should be consistent with national legislation and based on guidelines issued by competent authorities and international standards.

163. Supervisors should consider communicating with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities. This is particularly important where more than one supervisor is responsible for supervision (e.g., where the prudential supervisor and the AML/CFT supervisors are in different agencies or in separate divisions of the same agency). Multiple guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among securities providers. When possible, relevant regulatory and supervisory authorities should consider preparing joint guidance.

ANNEX A. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE SECURITIES SECTOR

Canada

164. As the AML/CFT supervisor in Canada, FINTRAC issues sector specific workbooks that help reporting sectors design a risk-based approach that is tailored to their business, including for securities: http://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-sec-eng.asp.

Guernsey

165. Guernsey is an international finance centre with a significant collective investment funds sector. There are more than 800 Guernsey domiciled funds authorised or registered by the Commission, which is the regulatory authority responsible for AML/CFT, conduct and prudential supervision of Guernsey's financial services sector.

166. Prudential and conduct supervision is undertaken by sector specific supervisory divisions with a dedicated AML/CFT supervisory division responsible for risk-based AML/CFT supervision across the industry as a whole. The AML/CFT supervisory division works closely with the relevant supervisory divisions. This collaboration includes sharing prudential, conduct and AML/CFT issues because of the crossover implications an issue may have for both supervisory teams, and in undertaking joint onsite inspections to optimise its resources.

167. The AML/CFT supervisory division also undertakes its own onsite inspections depending upon the firm's ML/TF risk profile, which is assessed annually utilising business and compliance data received from the firm, together with open source and confidential information available to the Commission, such as information from Guernsey's FIU. Each Guernsey fund must appoint a designated fund administration company which is responsible for discharging the fund's AML/CFT obligations, and in particular for the initial and ongoing customer due diligence on investors into the fund. Five of these administration firms administer approximately half of the assets under management in the funds sector. These administrators are subject to structured supervisory engagements, including onsite inspections at least every three to four years, under the Commission's risk based supervisory model.

168. Smaller administration firms are subject to less frequent structured supervisory engagements, the Commission uses thematic reviews to assess key issues on a firm and sector basis. As an example, the prudential and AML/CFT supervisory divisions undertook a joint thematic supervisory review of this sub-sector to analyse and assess the effectiveness of the governance, risk and compliance frameworks within these administration firms for managing both ML/TF and prudential risks. Whilst individual findings were raised with the relevant firm, anonymised findings together with examples of good and poor practice were published in a report on the thematic review to assist the whole industry in its development of effective AML/CFT controls. The Commission monitors the external use of its website and it recorded 801 online views of the report in the first two weeks after its publication. The thematic exercise also provided information for the Commission to use in its presentations to industry.

169. The AML/CFT supervisory division has also undertaken AML/CFT themed reviews on the provision of AML/CFT training within the industry.

Ireland

Central Bank of Ireland's AML/CFT Supervision of the Funds Sector

170. There are approximately 7,000 funds authorised by the Central Bank of Ireland (the Central Bank). Each fund is required to appoint an Irish authorised Fund Service Providers (FSPs) to administer the fund. The FSP is essentially the gatekeeper to the fund as it is the point of contact in the customer relationship between the investor and the fund and it is the FSP that provides the AML/CFT capability to the fund to discharge its AML/CFT obligations.

171. In order to utilise its supervisory resources in the most effective manner and maximise supervisory coverage, the Central Bank's AML/CFT supervisory strategy is to supervise funds through supervisory engagement of FSPs. Five FSPs account for almost 85% of the total amount of assets of Irish authorised funds. While the Central Bank's minimum AML/CFT supervisory engagement model provides for on-site inspections of FSPs at least once every five years, these five FSPs are subject to an on-site inspection at least once every three years. In addition, these five FSPs are also subject to an AML/CFT review meeting at least once every two years and are required to complete an online AML/CFT return at least once every two years. This supervision strategy enables the Central Bank to regularly assess the AML/CFT control framework of both the funds and the FSPs, through sample testing, interviews and reviews of policies and procedures. The Central Bank has also has a dedicated relationship manager for the funds industry to deal promptly and effectively with any issues that may arise on occasion.

172. The Central Bank's supervisory engagements are complemented by an AML/CFT communications and outreach programme to the funds sector. This includes presentations by the Central Bank at a number of industry events each year, as well as the publication of bulletins and reports that set out in aggregate and anonymised form the findings from the Central Bank's supervisory engagements. The publications also state the Central Bank's expectations around AML/CFT compliance.

Hong Kong, China

Securities and Futures Commission's AML/CFT Supervision Securities Sector

173. The Securities and Futures Commission (the "SFC") of Hong Kong conducts on-site inspections and employs various off-site monitoring tools to supervise licensed firms' compliance with AML/CTF requirements and monitor their ML/TF risks. The frequency, intensity and scope of the inspection and off-site monitoring carried out on an individual firm vary with, and are proportionate to, the risk level of the firm assessed based on a number of risk and impact factors. The SFC also conducts enforcement actions in relation to suspected breaches of AML/CFT legal and regulatory requirements and related internal control failures, for which a range of remedial measures and dissuasive sanctions may be imposed.

174. The SFC places emphasis on senior management responsibility (Manager-In-Charge or MIC), with detailed expectations regarding compliance and control functions that are relevant to MICs for AML/CFT as set out in the SFC's AML/CFT guidelines. If an MIC fails to ensure that the licensed firm complies with AML/CFT requirements, the failure may render the MIC liable to disciplinary sanctions (e.g. pecuniary fine and reprimand) imposed by the SFC. SFC's investigations will, whenever appropriate, focus

on the culpability of individuals with oversight of the AML/CFT function and other core functions.

175. The SFC places emphasis on sharing its supervisory observations, and signalling to all licensed firms its regulatory priorities and the focuses of compliance inspections. The goal is to promote and assist the efforts of licensed firms and their senior management in discharging their responsibilities. To this end, the SFC has initiatives in place to alert the industry of different areas of compliance concern from time to time. This includes communicating supervisory findings to the industry via circulars and seminars.

176. The SFC also provides transparency of its enforcement actions by issuing press releases on its enforcement actions. In disciplinary cases, a copy of the Statement of Disciplinary Action summarising the material facts and conclusion of a disciplinary action is available on the SFC's website.

Mexico

National Banking and Securities Commission's AML/CFT Supervision of Securities Sector and guidance provided for the implementation of the RBA

177. The National Banking and Securities Commission's (the "CNBV") of Mexico is responsible for the licencing and registration, prudential and AML/CFT supervision for the brokerage firms, investment funds and investment advisors. CNBV supervises other financial institutions as well, such as banks, savings and loan companies, money transmitters, among others.

178. The AML/CFT supervision consists of on-site inspections and off-site monitoring in order to verify the securities providers and intermediaries' compliance with AML/CFT requirements and monitor their ML/TF risks. The RBA on supervision is applied at different levels and stages of the supervision process. Off-site monitoring activities are carried out for all supervised entities. However, depending on their ML/TF level of risk, additional supervision measures are taken.

179. CNBV has a methodology that measures the ML/TF risks for all supervised entities considering the inherent risk for both ML/TF (two separate measures are performed, and the results are combined to obtain the entities ML/TF inherent risk), taking into account information provided by the entities themselves, the prudential supervisors and other authorities, such as the FIU, other supervisors and the federal law enforcement agency (PGR). The results of previous supervision actions are considered as the evaluation of their mitigating measures, which may reduce the inherent risk. Other factors are considered as risk intensifiers that may increase the inherent risk, such as the non-compliance with periodic obligations, findings indicated in the annual audit report, low quality of the STR's, obtaining at the end the residual risk for each entity.

180. The annual on-site visiting program takes into account the results from the aforementioned methodology and other additional factors, such as the systemic relevance and those related to special concerns from the AML/CFT and prudential supervision. With the resulting ratings, it is decided which entities will have stronger supervisory actions, starting with the on-site visits from the AML/CFT supervisors, on-site visits from the prudential supervisors including some specific AML/CFT topics, and continuing with other off-site additional monitoring programs.

181. Once the annual on-site visiting program is defined under an RBA, for each on-site visit it is necessary to identify the mitigating measures that are going to be revised

considering as well an RBA. A document called "entity's diagnostic" is executed at least one month in advance from the on-site visit including all the CNBV's available information as well as information from the FIU, and considering all the gathered elements, the visit strategy (intensity and scope) is defined. Additionally, during the on-site visit the selection of the entity's clients for a deeper revision is made based on the risk they represent for the entity itself, meaning another way to implement the RBA in the supervision process.

182. In 2017 the AML/CFT legal provisions in Mexico were modified in order to include as an obligation the design, implementation and assessment of an internal RBA for all entities supervised by the CNBV. In order to give guidance on the implementation of this new obligation, the CNBV has put into practice several actions:

- Issue a guideline in order to explain in a more detailed manner what is expressed in the legal provisions in terms of how to accomplish the design, implementation and assessment stages for their internal RBA.
- Organize forums by supervised sector in order to give some examples of how to apply the RBA given each sector's specific characteristics, including, products, type of clients, distribution channels and geographic areas of operation.
- Publish a video-tutorial with the most important information from the forums in the previous bullet, in order to have a wider range of reach among all the supervised entities, especially for those who were unable to assist to those forums.
- Carry out workshops where the supervisor's expectations regarding this new obligation are clarified and to perform some exercises for the design of the RBA methodology and supervisor's feedback regarding these exercises.
- Release the supervisor's on-site visit guidelines for all the supervised entities to make more transparent the supervision process and the entities could be aware of the supervisor's expectations in terms of compliance of all their AML/CFT obligations, especially regarding this new one.

ANNEX B. SUSPICIOUS ACTIVITY INDICATORS IN RELATION TO SECURITIES

This Annex provides examples of suspicious indicators in relation to securities, which may trigger filing of STRs and/or require additional CDD measures, including further investigation and ongoing monitoring, before a decision on filing is made by the securities provider. This is not an exhaustive list, and may not be relevant in all countries or circumstances.

I. Product/Customer Transactions suspicious activity indicators

1. Transactions do not have apparent economic rationale.

2. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.

3. A concentration ratio of transactions relating to a particular and/or higher risk jurisdiction that is notably higher than what is to be expected considering its normal patterns of trading of a customer.

4. Frequent trades resulting in losses for which the customer appears to have no concern.

5. Sudden spike in transaction volumes which deviates from previous transactional activity.

6. Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes.

7. A pattern of securities transactions indicating the customer is using securities trades to engage in currency conversion. Examples of securities that can be used in this manner include dual-currency bonds, American Depositary Receipts (ADRs) and foreign ordinary shares traded in the Over-the-Counter Market.

8. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.

9. Trading or journaling in the same security or securities between numerous accounts controlled by the same people (e.g. potential wash sales and/or directed trading).

10. Two or more unrelated accounts at the securities firm trade an illiquid or low priced security suddenly and simultaneously.

11. Purchase of a security does not correspond to the customer's investment profile or history of transactions (e.g., the customer may never have invested in equity securities or may have never invested in a given industry) and there is no reasonable business explanation for the change.

12. Transactions that suggest the customer is acting on behalf of third parties with no apparent business or lawful purpose.

13. Funds deposited for purchase of a long-term investment followed shortly by a customer request to liquidate the position and transfer the proceeds out of the account.

II. Distribution Channel suspicious activity indicators

1. Intermediaries whose transaction volume is inconsistent with past transaction volume.

2. A transaction pattern indicating a value of transactions just beneath any applicable reporting threshold.

III. Selected Indicators of Suspicious Trading or Market Manipulation

1. Making a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation.

2. A request is made to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.

3. Accumulation of stock in small increments throughout the trading day to increase price.

4. Engaging in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low priced securities.

5. Marking the closing price of a security.

6. Front-running suspected with regard to other pending customer orders.

IV. Suspicious Indicators Associated with Customer Due Diligence and Interactions with Customers

1. Customer has no discernible reason for using the securities provider's services or the firm's location (e.g., customer lacks ties to the local community or has gone out of the way to use the firm).

2. Customer's legal or mailing address is associated with other, apparently unrelated, accounts.

3. Locations of customer's address(es)/banks/financial institutions seem unconnected to the customer and little or no explanation can be given by the customer for the disparate addresses.

4. Customer is a trust, shell company, or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.

5. Customer is a legal person having issued bearer securities for a large part of its capital.

6. Customer is publicly known to have criminal, civil or regulatory proceedings against it for, corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is

known to associate with such persons. Sources for this information include news items or Internet searches.

7. Customer's background is questionable or differs from expectations based on business activities.

8. Customer has been rejected or has had its relationship terminated as a customer by other financial services firms.

9. Customer's account information reflects liquid and total net worth that does not support substantial account activity.

10. Customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

11. Non-profit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

12. Customer is reluctant to provide information in relation to its identity and/or transactions.

13. Customer is reluctant to provide information needed to file reports to proceed with the transaction.

14. Customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML/CFT policies.

15. Customer tries to persuade an employee not to file required reports or not to maintain the firm's required records.

16. Law enforcement or regulators have issued subpoenas and/or freeze letters regarding a customer and/or account at the securities firm.

17. Customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.

18. Customer does not exhibit a concern with the cost of transactions or fees (e.g., surrender fees, higher than necessary commissions) or of investment losses.

V. Suspicious Indicators in Deposits of Securities, Particularly Low Priced Securities; These Can Often Be Indicators of Low Priced Securities Fraud, Distribution of an Unregistered Offering, or Market Manipulation Schemes

1. Customer opens a new account and deposits physical certificates or delivers in shares electronically representing a large block of thinly traded or low-priced securities.

2. Customer has a pattern of depositing physical shares certificates or a pattern of delivering in shares electronically, immediately selling the shares and then wiring or otherwise transferring out the proceeds of the resale(s).

3. A sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.

4. The lack of a restrictive legend on shares physically or electronically deposited seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock, and/or the volume of shares trading.

5. Customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.

6. Customer's explanation of how the customer acquired the securities does not make sense or changes.

7. Customer deposits physical securities or delivers in shares electronically and requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

VI. Movement of Funds or Securities

1. The securities account is used for payments or outgoing wire transfers with little or no securities activities (i.e. account appears to be used as a depository account or a conduit for transfers with no reasonable business explanation for such).

2. Funds are transferred to financial or depository institutions other than those from where the funds were initially received, specifically when different countries are involved.

3. Customer "structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.

4. Customer engages in excessive journal entries of funds or securities between related or unrelated accounts without any apparent business purpose.

5. Payment by third party check or money transfer from a source that has no apparent connection to the customer.

6. Customer uses a personal/individual account for business purposes.

7. Payment to a third party to which the customer has no apparent connection.

8. Frequent transactions involving round or whole dollar amounts.

9. The customer requests that certain payments be routed through nostro [36] or correspondent accounts held by the financial intermediary instead of its own accounts.

[36] Nostro accounts are accounts that a financial institution holds in a foreign currency in another bank, typically in order to facilitate foreign exchange transactions.

10. Funds transferred into an account that are subsequently transferred out of the account in the same or nearly the same amounts, especially when origin and destination locations are high risk jurisdictions.

11. A dormant account suddenly becomes active without a plausible explanation (e.g. large amounts are suddenly wired out).

12. Frequent domestic and international automated teller or cash machine activity out of character with the customer's expected activity.

13. Many small, incoming wire transfers or deposits made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history. This may be an indicator of, for example, a Ponzi scheme.

14. Wire transfer activity, when viewed over a period of time, reveal suspicious or unusual patterns.

15. Transfers of funds or securities are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.

16. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.

17. Customer transfers/receives funds to/from persons involved in criminal or suspicious activities (as per the information available).

18. In/out transactions for substantial amounts on a short term basis.

19. Receipt of unexplained amounts, followed, shortly thereafter, by a request to return amounts.

20. Frequent transfers of securities' ownership.

21. Use of bearer securities with physical delivery.