FATF

GUIDANCE FOR A RISK-BASED APPROACH

SECURITIES SECTOR

OCTOBER 2018

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2018), *Guidance for a Risk-Based Approach for the Securities Sector,* FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html

Table of contents

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
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

Executive summary

1. The risk-based approach (RBA) is central to the effective implementation of the FATF Recommendations. It means that supervisors, financial institutions, and intermediaries identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.

2. The FATF RBA Guidance aims to support the implementation of the RBA, taking into account national ML/TF risk assessments and AML/CFT legal and regulatory frameworks. It includes a general presentation of the RBA and provides specific guidance for securities providers and for their supervisors. The Guidance was developed in partnership with the private sector, to make sure it reflects expertise and good practices from within the industry.

3. The Guidance describes various types of securities providers that may be involved in a securities transaction and their business models. It also sets out key characteristics of securities transactions that can create opportunities for criminals, and measures that can be put in place to address such vulnerabilities.

4. The development of the ML/TF risk assessment is a key starting point for the application of the RBA by securities service providers. It should be commensurate with the nature, size and complexity of the business. The most commonly used risk criteria are country or geographic risk, customer risk, product or service risk and intermediary risk. The Guidance provides examples of risk factors under these risk categories.

5. The Guidance highlights that it is the responsibility of the senior management of securities providers to foster and promote a culture of compliance as a core business value. They should ensure that securities providers are committed to manage ML/TF risks before establishing or maintaining business relationships.

6. The Guidance clarifies the role and responsibilities of intermediaries that may provide services on behalf of securities providers to customers of securities providers, customers of intermediaries or both. It highlights that the nature of the business relationship between the securities provider, the intermediary and any underlying customers will affect how ML/TF risks should be managed. This includes clarifying when the FATF's Recommendations on reliance apply.

7. The Guidance clarifies that when determining the type and extent of CDD to apply, securities providers should understand whether its customer is acting on its own behalf or as an intermediary on behalf of its underlying customers. Even when CDD is the responsibility of the intermediary, an understanding of the intermediary's customer base can often be a useful element in determining the risk associated with the intermediary itself. The level of understanding should be tailored to the perceived risk level of the intermediary.

8. Some business relationships in the securities sector might have characteristics similar to cross-border correspondent banking relationships; the Guidance also contains a description of how AML/CFT requirements apply to such relationships.

9. The Guidance highlights the importance of ongoing transaction monitoring to determine whether transactions are consistent with the securities provider's information about the customer and the nature and purpose of the business relationship. In case of any suspicions, security providers are required to report promptly their suspicions to the Financial Intelligence Unit. It provides up-to-date examples of indicators of suspicious activity in relation to securities sectors, which may trigger filing of STRs or additional CDD measures by securities providers, or further investigation or ongoing monitoring.

10. The Guidance stresses the importance of the group level approach to mitigate ML/TF risks, including the development of group-wide assessment of ML/TF risks and the sharing of relevant information between supervisors involved. It also highlights the importance of guidance and feedback from supervisors to securities providers on regulatory expectations and quality of reporting by securities providers. This will develop a shared understanding between the public and private sector. In this regard, the Guidance provides examples of supervisory practices of certain countries in the implementation of RBA in 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 a Risk-Based Approach: 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 on Private Sector Information Sharing
- the FATF Guidance for a Risk-Based Approach: Effective Supervision and Enforcement

relevant FATF typology reports, such as:

- the FATF Report: Money Laundering and Terrorist Financing in the Securities Sector (October 2009)

INTRODUCTION AND KEY CONCEPTS

Background and context

11. 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 the securities sector. 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 *FATF Report: Money Laundering and Terrorist Financing in the Securities Sector* (October 2009), which outlines vulnerabilities in the sector.

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

[2] www.fatgafi.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.

[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)].

13. The FATF adopted this updated RBA Guidance for the securities sector at its October 2018 Plenary.

Purpose of this Guidance

14. The purpose of this Guidance is to:

a) 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;

b) 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;

c) Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and

d) Support the development of a common understanding of what the risk-based approach to AML/CFT entails in the context of the securities sector.

Target audience, status and content of the Guidance

15. This Guidance is aimed at the following audience:

a) Countries and their competent authorities, including AML/CFT supervisors of the securities sector, and Financial Intelligence Units ("FIUs"); and

b) Practitioners in the securities sector (including securities providers and intermediaries, and external examiners for AML/CFT purposes).

16. 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.

17. 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 implementing a RBA; but it does not override the purview of national competent authorities. When considering the general principles outlined in the Guidance, national authorities should take into consideration their national context, including the supervisory approach and legal framework. Similarly, as with any application of the risk-based approach, securities providers should tailor their own policies and procedures to the risks they face and the jurisdictional requirements in which they conduct their business. In light of the complexity and scope of the sector, this Guidance may address issues not relevant to all securities providers, as it will by necessity, not address in detail, the entire spectrum of activities or entities operating in the sector.

18. This Guidance 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.

Scope of the Guidance: terminology, key characteristics and business models

Terminology

19. 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*.

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

a) Transferable securities, including equities and bonds or similar debt instruments;

b) Money-market instruments;

c) Investment funds, including units in collective investment undertakings;

d) 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;

e) Options, futures, swaps, forwards and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash;

f) Derivative instruments for the transfer of credit risk;

g) Financial contracts for differences; and

h) 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.

21. The above definition is neither rigid nor exhaustive. Differences exist in legal and regulatory definitions across different jurisdictions and the securities sector continues to evolve constantly with the introduction of new securities products and services. Further, national authorities should have the flexibility to identify providers of securities products and services, which should be subject to AML/CFT obligations, taking into account risk and context and their role in the securities sector.

22. In some countries virtual assets and the associated Initial Coin Offerings ("ICOs") are recognised as securities (and 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.

Key characteristics of the securities sector

23. Securities markets are often characterised by complexity, internationality, a high level of interaction, high volumes, speed and anonymity. Many of the core economic functions of securities markets are critical to efficient price-formation and capital allocation, which contribute to economic growth, job creation and overall prosperity. However, some of the same characteristics associated with the sector can create opportunities for criminals. *The FATF Report: 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 RBA are as follows:

a) The varying roles that securities providers and other intermediaries play in transactions; for example, a securities provider may be both an investment fund manager and a depository bank (see paragraphs 27-42 below);

b) Differences among jurisdictions in defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;

c) ML/TF risks stem mainly from the 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;

d) Global reach of the securities sector and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;

e) Ability to transact in securities products via an intermediary which may provide a relative degree of anonymity;

f) High liquidity of some securities products, which often enables their easy conversion to cash;

g) Complex products that may be offered before they are regulated (or not regulated at all) or rated for ML/TF risks (e.g. the crypto-assets mentioned above);

h) Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents, potentially limiting the ability of any one participant to have complete oversight of the transaction;

i) An often highly competitive and incentive-driven environment, which may lead to a higher appetite for risk, or failure to adhere to internal controls;

j) Pricing volatility of some products, particularly low-priced securities;

k) Transactions executed both on registered securities exchanges and elsewhere, such as over-the-counter (where parties trade bilaterally), and reliance on alternative trading platforms, electronic communication networks and internet-based trading;

l) Opportunity to use transactions in securities for generating illicit income within the sector, for example, market abuse or fraud; and

m) Challenges in pricing some securities products due to their bespoke nature or complexity.

24. Market abuse is a general term used to describe a wide range of types of unlawful behaviour in the financial markets including market manipulation, wash trading, insider trading, misappropriation, layering, unauthorized pooling, spoofing, front running and the like. Chapter 4 of the *FATF Report: 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.

25. 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 use in monitoring for suspicious activity for AML/CFT purposes. Such commonalities and efficiencies are to be encouraged so long as both market abuse and AML/CFT obligations are each fully met.

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

Securities providers (services and activities)

27. 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 members, prime brokers, global custodians, sub-custodians and depository banks including securities depository participants. This is not an exhaustive list of all securities providers, and in some instances a securities provider may assume more than one of the above roles. One characteristic, particularly of larger securities providers, is that they may perform a diverse set of activities through different legal divisions or entities within the same group. These

different group entities may be subject to different regulatory and statutory requirements and the group's risk-based approach will need to consider this carefully.

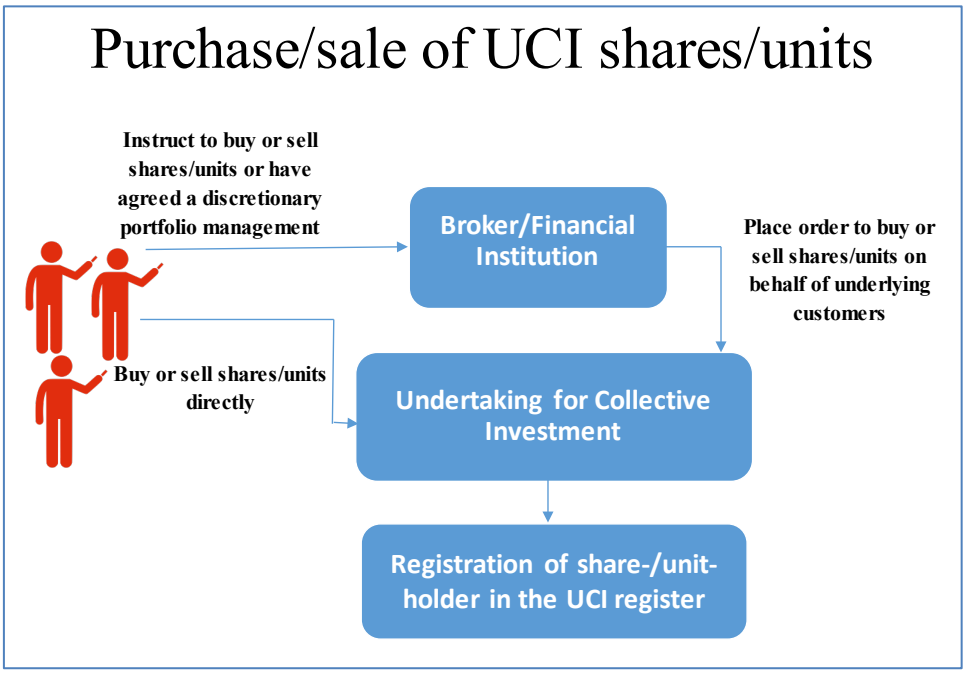
28. Securities providers offer various types of services, including capital market research and advisory, individual and collective portfolio management, investment funds distribution, order execution (trading in transferable securities), underwriting for issuers, private placements and other prospectus-exempt products, custody of client assets, lending money (providing margin) to clients and transfers of client cash (e.g. wire transfers). Mergers and acquisitions services and syndicate and secondary market financing are other types of securities services. 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. Different risks may arise when a securities provider offers customers, securities accounts with a wide range of transactional and cash-management services associated with securities. Regardless of the role, the securities provider must continually tailor its own RBA to assessing and managing ML/TF risk.

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

30. **Investment funds**, including undertakings for collective investment ("UCIs") and 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 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 the 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 another financial institution. When an intermediary's name is recorded in the investment fund's share/unit register but it is holding units for its underlying customers, the arrangement is often referred to as an "omnibus account".

31. See illustration below, which demonstrates in simple terms one of the many distribution arrangements for investment funds (also refer to section 7.1.3 of this Guidance).

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



32. Another type of securities provider is an **investment advisor**, which can be either an individual or a firm that gives advice about securities and financial planning to its customers, which may include individuals, institutions, trusts, or pooled investment vehicles.

33. A **broker** is a person or an entity that is in the business of buying and selling securities - stocks, bonds, mutual funds, and other investment products either on behalf of its customers or for its own account. A broker may have customers that are individuals or other legal entities (including financial institutions, corporate entities, partnerships and trusts).

34. Brokers serve retail customers and other institutions, such as pension plans, hedge funds, banks and other brokers. It is not uncommon that a number of different brokers are involved in a particular transaction, for example, an "**introducing broker**" may pass orders on to an "executing broker", who may execute the trade and give it up for clearing to a "clearing broker".

35. Securities providers known as **clearing members** or clearing brokers may provide record-keeping, confirmation, settlement, delivery of transactions and related functions associated with securities transactions, usually on behalf of other brokers, such as introducing or executing brokers.

36. **Institutional brokers** interact largely with large institutional clients and are often used to provide execution and custody services unaccompanied by investment advice. Customers of institutional brokers may and do use multiple institutional brokers to execute transactions.

37. **Prime brokers** provide execution, custody and other services to other financial institutions, such as hedge funds. This can include providing centralised clearing facilities for investment funds and allowing customers to borrow shares or money. Prime brokers may also act as record-keepers for other securities providers (e.g. investment advisors or investment managers) that may in turn be acting on behalf of customers' transactions.

38. Another type of securities provider, a **custodial broker-dealer**, 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").

39. The **global custodian** provides safekeeping and settlement "custody services" for fund-managers, their underlying funds, asset managers and other institutional clients across multiple markets globally through a network of relationships with sub-custodians, banks, national and international central securities depositories (CSDs).

40. A **sub-custodian** provides safekeeping, clearing and settlement custody services in a domestic or international market on behalf of its customers. Although often employed by a global custodian, the sub-custodian, also referred to as an agent bank, might also service brokers and banks.

41. A **central securities depository** (CSD) provides securities accounts and, in many countries, operates a Securities Settlement System. A CSD also provides central safekeeping and asset servicing and plays an important role in helping to ensure the integrity of securities issues. The CSD will service many customers including sub-custodians, banks, brokers, global custodians, prime brokers, and issuers.

42. The size and complexity of securities providers vary significantly and as discussed above, they use various business models and may play different roles in different transactions. 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 have more complete transparency relating to a transaction. Thus, a securities provider should appreciate that it may not have a full picture of the entirety of business occurring through it and should therefore conduct an initial and ongoing risk assessment of its customers and activities to best understand and then mitigate any ML/TF risks identified.

Intermediaries

43. 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 securities provider, a customer of the intermediary, or a customer of both.

44. Services provided by these intermediaries could include performing certain aspects of CDD, which are relied upon by a securities provider (reliance model - see paragraphs 114-116 for further description). Services may also include distribution services for selling securities products on behalf of a securities provider.

45. The distribution of securities products and services can also 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.

46. 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. Indeed, an intermediary can be and very often is a securities provider itself, providing securities services within a chain of multi-step transaction.

47. All these different models and business practices may pose different ML/TF risks and require different approaches to risk mitigation.

48. 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 highlights the importance of securities providers' understanding of how their business arrangements raise ML/TF risks both directly (e.g. through transactions executed by customers) and 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). Securities providers should implement risk-sensitive measures to mitigate the ML/TF risk faced by them.

International provision of securities products and services

49. 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 the FATF 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.

50. 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.

51. This Guidance provides more detail on the recommended actions for securities providers and competent authorities in Sections II and III.

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

WHAT IS THE RBA?

52. The RBA to AML/CFT means that countries, competent authorities and financial institutions[5] should 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.

53. When assessing ML/TF risk, 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[6]. For securities providers, this will require an understanding of the ML/TF risk faced by the sector as well as specific products and services, customer base, the capacity in which their customers are operating (e.g. on their own behalf or on behalf of underlying customers), jurisdictions in which they operate and the effectiveness of risk controls 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 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/TF in isolated instances.

54. A RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low[7].

THE RATIONALE FOR A NEW APPROACH

55. 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.

56. 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 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[8].

---

[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, paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

[7] 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 (paragraph 6, 11 and 12) and INR.10 paragraph 16 and 21.

[8] R.1.

The RBA is an over-arching requirement applicable to all relevant FATF Recommendations.

57. 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.

58. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards[9].

APPLICATION OF THE RISK-BASED APPROACH

59. R.1 sets out the scope of the application of the RBA. It applies in relation to:

a) 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[10], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF.

b) 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

c) 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 the required measures has to be applied, but they may be applied more narrowly, less frequently, or in a reduced way [11].

[9] 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).*

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

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

CHALLENGES

60. Implementing a RBA can present a number of challenges:

Allocating responsibility under a RBA

61. 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 all relevant national risk assessments in line with R.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 (e.g. varying the degree or frequency of ongoing monitoring), although national law or regulation might not prescribe exactly how these higher risks are to be mitigated[12].

62. Securities providers should have the flexibility in deciding the most effective way to address other risks, including those identified in the national risk assessment or by the securities providers. The securities providers' strategy to mitigate these risks must take into account the applicable national legal, regulatory and supervisory frameworks. When deciding the extent to which securities providers may be permitted to independently mitigate risk, countries should consider 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 effectively supervise securities providers and take measures to address any failure by securities providers to do so.

63. 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[13].

64. 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[14]. Nonetheless, countries and competent authorities should take steps to effectively supervise all entities covered by AML/CFT requirements.

---

[12] R.1.

[13] 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 (financial sector assessment program) reports.

[14] See FATF Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement.

Identifying ML/TF risk

65. 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 basis, and to develop innovative techniques to combat ML/TF[15]. 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[16]. 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.

Assessing ML/TF risk

66. 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 individual securities providers, the securities sector, large- scale financial institutions, and the national economy, if they did occur[17]. 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.

67. 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 (e.g. medium-high, low-medium). 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.

68. Assessing and understanding risks means that competent authorities and securities providers should have skilled and trusted personnel, proportionate to the size and ML/TF risk and recruited through fit and proper tests, where appropriate. This also requires such personnel to be technically equipped to carry out their responsibilities.

[15] See R.18, R.20, R.21 and FATF Guidance on Private Sector Information Sharing.

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

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

Mitigating ML/TF risk

69. 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 enhanced measures should be taken to manage and mitigate situations in which the ML/TF risk is higher; and that, correspondingly, in lower risk situations, less stringent measures may be applied[18]:

a) 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 stand to benefit from the exemption. The nature and complexity of the securities sector mean that this exemption often will not apply

b) Securities providers looking to apply less stringent 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[19].

Developing a common understanding of the RBA

70. The effectiveness of a 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. The legal and regulatory framework should spell out the degree of discretion appropriate for financial institutions in the sector to assume. Competent authorities and supervisors in particular should 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 essential for the successful implementation of a RBA.

71. Competent authorities should acknowledge that in a risk-based regime, not all securities providers will adopt the same AML/CFT controls and that relatively isolated incidents of insignificant risk should 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. They should be able to explain to their supervisors the effectiveness of their AML/CFT controls and how those controls are commensurate with the risks identified.

---

18 Subject to the national legal framework providing for Simplified Due Diligence.

19 For example, R.10 on Customer Due Diligence and INR.10.

SECTION II – GUIDANCE FOR SECURITIES PROVIDERS AND INTERMEDIARIES

72. This section should be read in conjunction with the *FATF Report on Money Laundering and Terrorist Financing in the Securities Sector* (October 2009), especially the summary of Chapter 3 highlighting 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.

RISK ASSESSMENT

73. Combating ML/TF 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 because 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.

74. The risk assessment should be properly documented, regularly updated and communicated to the relevant securities provider's senior management. In conducting their risk assessments, securities providers should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate these risks[20]. This may include consideration of the risk and threat assessments, crime statistics, typologies, risk indicators, red flags, guidance and advisories issued by inter-governmental organisations, national competent authorities and the FATF, and AML/CFT mutual evaluation and follow-up reports by the FATF or associated assessment bodies. Many governments and authorities carry out ML/TF risk assessments for their jurisdictions, and securities providers should take these into account where relevant, when they are published or otherwise communicated. Furthermore, in identifying and assessing indicators of ML/TF risk to which it is exposed, a securities provider should consider a range of factors including:

a) The nature, diversity and complexity of its business, products and target markets;

b) The proportion of customers identified as high risk;

c) The jurisdictions in which the securities provider is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other

[20] 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.

risk factors such as the prevalence of crime, corruption, or financing of terrorism, the general level and quality of the jurisdiction's prosecutorial and law enforcement efforts related to AML/CFT, the regulatory and supervisory regime and controls and transparency of beneficial ownership;

d) 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/CFT obligations, the complexity of the transaction chain (e.g. layers of distribution and sub-distribution, type of distributors such as independent financial advisors, investment advisors) and the settlement systems used between operators in the payment chain, the use of technology and the extent to which intermediation networks are used;

e) The internal and external (such as audits carried out by independent third parties, where applicable) control functions and regulatory findings; and

f) The expected volume and size of its transactions, considering the usual activity of the securities provider and the profile of its customers[21].

75. Securities providers should review their assessments periodically and when their circumstances change or relevant new threats emerge. Securities providers should consider internal feedback within their organization, including from those who interact with customers, compliance risk management, and internal audit departments (where relevant), in performing their periodic risk assessments.

76. ML/TF risks may be measured using various methods. The use of risk categories enables securities providers to manage potential risks by subjecting 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.

77. 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 risk may vary from one institution to another, depending on their respective circumstances and risk management framework. Securities providers must comprehensively review all risk factors relevant to their business, including how certain factors may interplay and have an amplifying effect. For example, the risks inherent in an under-developed securities sector could be amplified by regional risks (if it is located, e.g. in an area where there is high incidence of drug trafficking). Consequently, securities providers should determine the risk weights and at the same time, parameters set by law or regulation may limit a business's discretion.

78. 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:

[21] See R.1 (c1.10 and c.1.11), INR.1 and R.10.

Country/Geographic risk

79. There is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which the securities provider or intermediary operates, such as a particular country, geographic area or border region within a country, 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:

a) Countries/areas identified by credible sources[22] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b) 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.

c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation.

d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

Customer/Investor risk

80. Securities providers should determine whether a particular customer/investor[23] poses higher risk and analyse the potential effect of any mitigating factors on that assessment. Such categorisation may be due to a 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:

a) Customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT regime and is not engaging in remediation to improve its compliance.

b) Customer is a PEP or customer's family members or close associates are PEPs (including where a beneficial owner of a customer is a PEP) as covered under R.12.

---

22 "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.

23 The use of the term "customer" covers "customer/investor" throughout the guidance.

c) 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).

d) Customer resides in countries considered to be uncooperative in providing beneficial ownership information.

e) Customer acts on behalf of a third party and is either unwilling or unable to provide consistent information and complete documentation thereon.

f) Customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or to financial crimes.

g) 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.).

h) Customer is also a securities provider, acting as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak AML/CFT oversight.

i) Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business

j) The number of STRs and their potential concentration on particular client groups.

k) Customer is a legal entity predominantly incorporated in the form of bearer shares.

l) Customer is a legal entity whose ownership structure is unduly complex as determined by the securities provider or in accordance with any regulations or guidelines.

m) Customers who have sanction exposure (e.g. have business/activities/transactions).

n) Customer has a non-transparent ownership structure.

Product/Service/Transactions risk

81. 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 or clear trades, handling the movement of funds or securities for the customer and settling a customer's transactions and liabilities. The securities provider may also offer brokerage accounts as a custodian of a customer's assets. Transactions may be conducted on a regulated exchange or other market or they may be conducted between parties directly. A securities provider should assess, using a RBA, the extent to which the offering of its products and services presents potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

82. 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:

a) 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).

b) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions.

c) Products with unusual complexity or structure and with no obvious economic purpose.

d) Products or services that permit the unrestricted 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.

e) Use of new technologies or payment methods not used in the normal course of business by the securities provider.

f) Products that have been particularly subject to fraud and market abuse, such as low-priced securities.

g) The purchase of securities using physical cash.

h) Offering bank-like products, such as check cashing and automated cash withdrawal cards.

i) Securities-related products or services funded by payments from or instructions given by unexpected third parties, particularly from higher risk jurisdictions.

j) Transactions involve penny/microcap stocks.

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

a) A request is made to transfer funds to a higher risk jurisdiction/country/corridor without a reasonable business purpose provided.

b) 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.

Distribution channel risk

84. 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.

85. A securities provider that distributes 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 in 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.

86. A securities provider should analyse the specific risk factors, which arise from the use of intermediaries and their services. 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, whereas in other cases intermediaries may also use the products and services for their underlying customers (e.g. where the business relationship is established between intermediary and customer).

87. Regardless of the model, a securities provider should understand who the intermediary is and perform a risk assessment on the intermediary prior to establishing a business relationship. Securities providers and intermediaries should establish clearly their 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 the following factors, to the extent that these are relevant to the securities providers' business model:

a) Intermediaries suspected of criminal activities, particularly financial crimes or association with criminal associates.

b) Intermediaries located in a higher risk country or in a country with a weak AML/CFT regime.

c) Intermediaries serving high-risk customers without appropriate risk mitigating measures.

d) Intermediaries with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law enforcement.

e) Intermediaries that have failed to attend or complete AML/CFT training programmes requested by the securities providers.

f) 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.

RISK MITIGATION

88. 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 more resources to mitigating their most significant risks.

Customer/Investor due diligence

CDD general considerations

89. 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 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 a customer; (b) when carrying out occasional transactions above the applicable monetary threshold; (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, R.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.

Initial and ongoing CDD

90. Securities providers should develop and implement policies and procedures to mitigate the ML/TF risks identified through their individual risk assessment. In light of that assessment, CDD processes should help securities providers understand who their customers are by gathering information on what they do and why they require their services. The initial stages of the CDD process should 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.

91. Based on information obtained in the CDD process, securities providers should prepare a customer risk profile. Customer risk profiles should be informed by the FATF Standards, including those covered in INR.10, R./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 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 (e.g. customers with similar income range, or conducting similar types of securities transactions). On the basis of their risk assessment, securities providers should periodically update customer risk profiles, which should help them apply the appropriate level of CDD.

92. 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. 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.

93. When designing CDD procedures and conducting CDD on customers, securities providers should, where appropriate, consider the following issues:

- **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. This includes verifying the authorisation of persons purporting to act on behalf of the customer, their identification and verification on a risk-sensitive basis and understanding the role the securities provider plays. In higher risk situations, obtaining further information for ongoing monitoring of the business relationship and detection of potentially suspicious activity may be needed.
- **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 to undertake reasonable steps to verify the identity of beneficial owner(s). Securities provider should also consider whether the opacity of the ownership structure or the identity of one or more beneficial owners is an indicator of elevated risk and whether it is a cause or not for not performing the transaction or terminating the business relationship and considering making a suspicious transaction report.
- **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.

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

95. 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 associated with the individual business relationship. 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 or decreased where the associated risk is lower.

96. A securities provider should conduct CDD on an initial and ongoing basis. A securities provider should endeavour to be aware of material changes to the customer's legal form, beneficial ownership and 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.

The securities provider's customer

97. 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 31, which provides an example of investment funds where the customer may be direct or indirect. Also, for a discussion of issues particular to similar correspondent relationships in the cross-border context, refer to section 7.1.5 of this Guidance.

98. The business relationship between the securities provider, the intermediary and any underlying customers, including the degree of transparency the securities provider has into any underlying customers and their transactions will affect a number of AML/CFT obligations and outcomes, such as who is responsible for conducting CDD, the securities provider's risk assessment of the intermediary and the securities provider's ability to monitor transactions associated with the intermediary and its underlying customers.

99. When determining the type and extent of CDD to apply, a securities provider should be clear as to whether its customer is acting on its own behalf or as an intermediary on behalf of its underlying customers. Even when CDD is the responsibility of the intermediary, an understanding of the intermediary's customer base can often be a useful element in determining the risk associated with the intermediary itself; the level of understanding obtained should be tailored to the perceived risk level of the intermediary.

100. While a detailed analysis of the wide variety of intermediary and customer relationships that occurs in the securities sector is beyond the scope of this Guidance, a brief discussion of the distribution of investment funds may illustrate some common themes and concerns. In this context, the CDD measures an investment fund should take will depend on how the ultimate customer invests in the fund. Depending on how the investment fund is sold, with whom the business relationship is established or who is registered in the fund's share/units register, the investment fund may be required to treat an underlying investor as its customer or the 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.

101. Securities providers should also obtain (and intermediary should provide) information about the intermediary's AML/CFT controls, including information regarding the intermediary's risk assessment of its underlying customer base and its implementation of risk mitigation measures.

102. The above requirements may be adapted to particular conditions (e.g. additional onsite control or other more thorough controls when an intermediary is a non-regulated or non-supervised entity or is located in a country presenting high ML/TF risks).

Enhanced CDD ("EDD") and simplified CDD ("SDD")

103. 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.

104. 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 is not generally appropriate, unless there is proven low risk of ML/TF. SDD measures are also not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

105. One example of when SDD measures may generally be appropriate is a pension product funded directly from a reputable company's payroll as such a product may present a lower ML/TF risk compared to other products. Conversely, EDD measures must be required for a PEP customer since such a customer presents heightened risks. Illustrative examples of both SDD and EDD measures are detailed below. However, these examples are intended to form a non-exhaustive list, and financial institutions are encouraged to apply a risk-based analysis that takes account of the particular circumstances of each case.

Box 1. Non Exhaustive List of 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
- Carrying out additional searches focused on financial crime risk indicator (i.e. negative news screening) to better assess the customer risk profile
- Obtaining additional or more particular information about the intermediary's underlying customer base and its AML/CFT controls
- 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 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 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

Correspondent Relationships [24]

106. INR.13 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. Because certain relationships in the securities sector have characteristics similar to cross-border correspondent banking relationships, they are addressed in this Guidance.

107. A typical cross-border correspondent relationship in the securities sector 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. One example of these types of relationships could be between a global securities firm (correspondent) executing securities transactions on a stock exchange for a cross-border intermediary, acting as a respondent for its underlying local customers, subject to complying with R.13 requirements.

108. Not all cross-border correspondent relationships pose the same level of ML/TF risk and the securities providers should adjust the type and extent of CDD measures to account for the risk posed by the respondent. The correspondent institution should monitor the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile (i.e. compliance with AML/CFT measures and applicable targeted financial sanctions), any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent 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.[25]

109. 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.
- Additional due diligence on the correspondent relationship with the respondent, as described below.

110. In accordance with R.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

24 FATF Guidance on correspondent banking services (October 2016).

25 See Paragraph 3 of the FATF Guidance on correspondent banking services (October 2016).

supervision, including whether and when it has been subject to targeted financial sanctions, a ML/TF investigation or regulatory action;

- Assess the respondent's AML/CFT controls. The assessment should include confirming that the respondent institution's AML/CFT controls are subject to independent audit (which could be external or internal). A more detailed/in-depth review should be conducted for higher risk relationships, possibly including reviewing the independent audit, interview of compliance officers, a third party review and potentially an onsite visit;
- Obtain approval from its senior management before setting up a correspondent relationship;
- Clearly understand the respective AML/CFT responsibilities of each institution.

111. In the case of such relationships, the correspondent generally does not have direct relationships with the customers of the respondent. There is no expectation or requirement for the correspondent to apply CDD on a respondent's customer, which is, instead the responsibility of the respondent. Nonetheless, it is consistent with the risk-based approach for the correspondent to have some general sense of the respondent's customer base as part of ascertaining the risks associated with the respondent itself.

112. 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.

113. 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.

Reliance on third parties

114. In accordance with R.17 and where permitted by local legislation, a securities provider may reasonably rely on third parties for performing some elements of initial CDD (identification of customer, identifying and taking reasonable measures to verify identification of beneficial owner and understanding the purpose and intended nature of business relationship). However, it may not rely on such parties to perform ongoing monitoring, ongoing due diligence and scrutiny of transactions. The term 'third parties' means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under R.17. Specifically the securities provider should complete appropriate due diligence on the third party to determine whether reliance can be placed on the AML/CFT risk and control framework of financial institution or DNFBP and whether they are based in a country whose risk has been assessed by the securities provider (in accordance with R.17(1) (c and d).

115. 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 satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the relied upon institution upon request and without delay.

116. Where appropriate, securities providers should ensure that formal agreements, which clearly set out the terms and conditions, including the roles and responsibilities of both the securities provider and the institution relied upon, are in place.

Outsourcing

117. The reliance model above can be contrasted with an outsourcing or agency scenario, where the outsourced entity conducts CDD on behalf of the securities provider, in accordance with the procedures of securities provider and under its instructions. In such case, the securities provider is the principal while the outsourced entity acts as its agent.

118. 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 relevant terms and conditions, including the roles and responsibilities of both the outsourced entity and the securities provider, are in place.

119. The ultimate responsibility for CDD and/or ongoing monitoring remains with the securities provider; again, it cannot delegate responsibility. In this regard, the securities provider should implement appropriate processes to monitor that the outsourced entity is performing effectively in accordance with the instructions set by the securities provider.

Electronic wire transfers requirements

120. R.16 establishes the requirements for countries with respect to wire transfers. R.16 apply to both cross-border wire transfers and domestic wire transfers[26]. 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. Countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer and beneficiary information is not required unless there is an ML/TF suspicion[27]. 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

26 INR.16 paragraph 3.

27 INR.16 paragraph 5.

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.

121. 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 taking the appropriate follow-up actions[28]. 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.

122. 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.

Suspicious transaction monitoring and reporting

Risk-based monitoring

123. 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 fund movements. Monitoring also involves identifying changes to the customer risk profile - for example, the customer's behaviour, use of products and the value involved, and keeping this information up-to-date, which may trigger the application of enhanced CDD measures. When suspicious activity or high-risk behaviour is identified, appropriate steps should be taken in a timeline commensurate with the risk.

124. Transaction monitoring is essential for identifying suspicious transactions. Transactions that are not in line with the customer's risk profile, that exhibit red flags of established money laundering typologies, or that deviate from the usual pattern, may be potentially suspicious. Securities providers may also draw upon surveillance frameworks and tools used to detect predicate offences to money laundering, such as market abuse and insider dealing in securities, to identify suspicious transactions. Integration of existing data sets more efficiently into AML/CFT framework can produce more effective results.

125. In many wholesale business relationships, such as principal to principal execution-only, the securities provider will generally have limited visibility of the end-to-end transaction; it is also typical for the underlying instructing party to have multiple brokers and deal in various products and asset classes, meaning that securities providers will only have visibility of a part of the overall trading activity. In such circumstances, effective transaction monitoring measures are likely to consist of leveraging existing market surveillance controls, rather than implementing electronic transaction monitoring systems similar to those in retail relationships. For example, in wholesale markets, securities providers may reasonably determine that, given the

[28] INR.16 paragraph 18 and 22.

difficulties in developing meaningful rules for electronic monitoring, it may be appropriate to implement alternative methods of monitoring. Whatever the approach taken, the securities provider should be able to demonstrate the rationale for their monitoring strategy.

126. A customer may transact in multiple jurisdictions and with multiple financial firms, which perform a variety of activities in relation to securities transactions. A securities provider may consider the following to determine the nature and extent of monitoring activity:

a) 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;

b) The risk and complexity of products offered to customers;

c) The volume and frequency of transactions processed by the securities provider; and

d) The execution, clearing or settlement processes facilitated by the securities provider, including consideration as to whether payments to third parties are permitted.

127. Transaction monitoring should be carried out on an ongoing basis and may be triggered by specific and unusual transactions. For example, a sudden spike in trading volumes for a particular issuer can be a red flag of potentially suspicious activity, such as a fraud associated with low priced securities. However, market events, like corporate announcements, news or rumours on likely mergers or acquisitions may also contribute to unusual trading patterns; this means that such a sudden spike in trading volume may not be suspicious upon further consideration, but instead was simply a red flag worthy of further inquiry. Therefore, in conducting effective transaction monitoring, the securities provider should take into account such market events.

128. 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. For example, having less visibility into the underlying customer of an intermediary might increase the risk profile of the intermediary itself. 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.

129. Monitoring under a RBA allows securities providers to create internal thresholds based on a range of factors, such as transaction number or value to determine which activities should 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. Monitoring system should flag unusual movements of funds or transactions for further analysis and scrutiny in a timely manner for determining as to whether the funds movements or transactions are suspicious.

130. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be readily explicable. If a securities provider establishes different customer segments for monitoring, it 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.

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

132. Securities providers should properly document, retain and communicate to the relevant staff the results of their monitoring and any queries raised and resolved.

Reporting suspicious activity

133. 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.

134. Transactions or movements of funds that are considered suspicious should be promptly reported to the FIU, in the manner specified by the competent authorities. Securities providers' processes 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.

135. Some jurisdictions require that suspicious market abuse (see paragraphs 24-26 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.

INTERNAL CONTROLS AND COMPLIANCE

Internal controls and governance

136. Adequate internal controls are critical for an effective AML/CFT 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 for identifying, assessing, and monitoring ML/TF risks where they operate. Securities providers should 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.

137. 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.

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

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

a) 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 significant ML/TF risks; and
   - Business relationships will not be established when the ML/TF risks cannot be mitigated and managed.

b) 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 ML/TF risks faced by the securities provider. Where applicable, these processes should link the board of directors, the top AML/CFT compliance officer, any relevant committee (e.g. the risks or ethics/compliance committee), the information technology unit and each of the business areas;
   - Help to determine the measures needed to mitigate the identified ML/TF risks and the extent of residual risk the securities provider is ready to accept; and
   - Allocate adequate resources for the securities provider's AML/CFT function.

140. Senior management should not only be aware of 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:

a) Understands the regulatory and supervisory requirements where the securities provider operates;

b) 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;

c) Receives sufficient and objective information to understand whether the securities provider's AML/CFT controls are effective;

d) Receives updates on government enforcement actions and other communications related to the AML/CFT obligations of securities providers and ML/TF risks; and

e) Ensures that processes are in place to timely escalate important decisions that directly affect the ability of the securities provider to address and control risks.

141. A sufficiently senior person within a securities provider should have the responsibility to ensure the effectiveness of AML/CFT controls. This is to highlight the importance of ML/TF risk management and compliance and for bringing ML/TF issues to senior management's attention. This includes the appointment of a skilled compliance officer at the senior management level[29]. 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).

142. R.18 requires financial institutions to have an independent audit function to test the effectiveness of its AML/CFT programme, policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestic and cross-border. Such independent testing should allow senior management to validate the development and operation of the risk assessment and management processes and internal controls, in order to ensure that the adopted measures reflect 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 design, implementation or operation of the securities provider's AML/CFT compliance programme. The testing should be risk-based; evaluate the adequacy of the securities provider's AML/CFT policies and programme and the quality of risk management for its operations, departments and subsidiaries; and cover all activities.

143. 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.

Compliance controls

144. 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.

145. 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. This includes the diversity of its operations, geographical location, customer base, 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 through intermediaries, third parties, or in a non-face-to-face setting without appropriate mitigating measures).

29 INR.18.

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

a) Place priority on the securities provider's operations (products, services, customers and geographic locations) that are more vulnerable to abuse.
b) Provide for regular review of the risk assessment and management processes, taking into account the environment within which the securities provider operates and the activity in those locations in which it operates.
c) Provide for an AML/CFT compliance function and review programme that includes the testing of key components.
d) Verify that adequate risk assessment and controls are in place before offering new products or services.
e) Regularly inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports.
f) Provide for programme continuity despite changes in management or employee composition or structure.
g) Focus on complying with applicable regulatory requirements on record keeping and reporting for AML/CFT compliance and timely response to changes in regulations.
h) Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
i) Provide for adequate management and oversight of its intermediaries, including initial intermediary due diligence, oversight of AML/CFT training, and ongoing risk-based monitoring.
j) 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.
k) Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
l) Ensure that staff or firm performance is not the driver for taking disproportionate ML/TF risks.
m) Provide for appropriate initial and refresher training to for all relevant staff.
n) Provide for initial and refresher training for intermediaries, as applicable, at appropriate intervals.

Vetting and recruitment

147. 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.

148. 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's roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

Training and awareness

149. The effective application of AML/CFT policies and procedures depends on the understanding of securities providers' staff of 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. Staff should receive AML/CFT training, which should be:

a) 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;

b) Obligatory for all appropriate staff, including senior management;

c) 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;

d) 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;

e) Regular, relevant, and not a one-off exercise when staff are hired, in line with INR.18; and

f) Complemented by AML/CFT information and updates that are disseminated to relevant staff, as appropriate.

150. 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. Training may also be provided by a third party, though the securities provider remains responsible for the quality of the training.

SECTION III – GUIDANCE FOR SUPERVISORS

151. The RBA to AML/CFT aims to develop prevention or mitigation measures that are commensurate to the ML/TF risks identified. For supervision, this applies to the way supervisory authorities allocate their resources and conduct supervisory tasks to facilitate the application of a risk-based approach by securities providers.

THE RISK-BASED APPROACH TO SUPERVISION

152. 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).

Understanding ML/TF risk

153. Supervisors should understand the ML/TF risks to which the securities sector is exposed[30], and the ML/TF risks associated with securities providers, both at an individual firm level and a financial group level, and the different securities sub-

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

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 bodies.

154. 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.

155. 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 effectiveness 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.

156. Some of this information should be obtained from the supervised entities (e.g. on the size, business model, location and nature of business). 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[31]. In some jurisdictions, this may involve information sharing and collaboration between prudential and AML/CFT supervisors or between different AML/CFT supervisors, especially when the responsibilities belong to two or more separate agencies.

157. Information from the securities providers' 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.

158. 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 new threats or vulnerabilities emerge. These could include, for example, new products and delivery channels that pose ML/TF risks, or the absence of local regulations to govern them sufficiently.

Mitigating ML/TF risk

159. 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, 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.

[31] As specified in ICP 3.

160. 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 to prevent criminals or their associates from holding a significant or controlling interest in a securities provider. 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 approve applications 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 have both on-site and off-site access to all relevant risk and compliance information. 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. They should combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. due to information received from law enforcement or whistle-blowers). General supervisory findings on thematic areas (e.g. focused reviews of particular products or services or types of providers or customers, or particular areas of interest such as beneficial ownership, distribution channels used etc. by securities providers) may also inform these supervision decisions.

d) **Adjusting the intensity of AML/CFT supervision**: supervisors should determine the scope or level of supervision in line with the risks identified in order to assess the adequacy of a securities provider's policies and procedures. Examples of more intensive supervision could include detailed review of the implementation and adequacy of the provider's risk assessment, files on CDD and reporting, record-keeping policies and processes and internal auditing. This may also include interviews with operational staff, senior management and the board of directors and AML/CFT assessment in particular lines of business.

161. 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 framework remains adequate. Whenever appropriate, these findings should also be communicated to the provider to enable them to enhance their RBA.

162. In line with R.26 and the application of the International Organisation of Securities Commissions (IOSCO) Core Principles relevant for AML/CFT[32], 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

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

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.

163. FATF R.27 and R.35 requires supervisors to 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, including a range of supervisory interventions; remedial/corrective actions to ensure proper and timely correction of identified deficiencies and 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.

AML/CFT supervision of securities providers in a cross-border context

164. For cross-border supervision, 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.

165. 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 inform the host supervisor that the financial institution may be subject to additional supervisory actions. This could result in enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host country.

166. In adopting a RBA to supervision, countries and competent authorities may consider allocating supervised entities sharing 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 intermediary within a grouping changes, the supervisor may reassess the supervisory approach, which may include removing the securities provider or intermediary from the grouping.

SUPERVISION OF THE RISK-BASED APPROACH

General approach

167. Supervisors should encourage and monitor securities providers' adoption of a 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.

168. Supervisors should note that under the RBA, particularly in the securities sector, given the diversity in size, scale of operations, 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; proportionality is an important element to be considered. In evaluating the adequacy of their RBA, supervisors should take into consideration the merits of these differences.

169. The securities sector is 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.

170. 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, sub-sector 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 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. In assessing the adequacy of resources, 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 an effective RBA, supervisors should also focus on assessing the quality of the securities providers' controls and effectiveness of their implementation to mitigate the ML/TF risks. Supervisors should clearly articulate and communicate their expectations, including the necessary rectification measures where there are deficiencies in providers' controls.

171. Examples of supervisory practices adopted in a number of countries for implementation of the RBA in the securities sector are set out in Annex A.

Training

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

173. Training should allow the 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 at the national level in case of multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

174. 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:

a) General AML/CFT issues;

b) Business models of various sub-segments of the securities sector (e.g. broker-dealers, fund managers) and the associated ML/TF risk issues;

c) 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;

d) International regulatory actions, such as economic sanctions;

e) National and international supervisory cooperation mechanisms; and

f) 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).

Guidance and Feedback

175. 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.

176. 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 with any guidelines issued by competent authorities and international standards.

177. Supervisors should communicate 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.

178. To the extent possible, supervisors and FIUs should provide timely feedback to securities providers on effectiveness of their monitoring/reporting systems, quality of STRs filed and AML/CFT controls in general. A well-defined and institutionalised feedback mechanism can enhance the effectiveness of the monitoring and surveillance system to capture as many suspicious transactions as possible while efficiently avoiding too many false-positives. Guidance on potential risk indicators in the securities sector, in consultation with the industry, where feasible, can also be considered.

ANNEX A. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RBA IN THE SECURITIES SECTOR

Canada

179. 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

180. 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.

181. 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.

182. 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.

183. 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.

184. 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

185. 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 often the point of contact in the customer relationship between the investor and the fund. When appointing an FSP, the fund will typically contract the FSP to provide certain AML/CFT services to the fund; however this does not absolve the fund from its own obligations.

186. 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.

187. 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

188. 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.

189. 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.

190. 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.

191. 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.

Luxembourg

192. Luxembourg Investment funds and their Luxembourg Investment Fund Managers as well as service providers established in Luxembourg are obliged entities under the applicable AML/CFT framework. The CSSF is the competent supervisory authority for all the entities falling under its remit. The Luxembourg investment fund industry is notably characterised by its cross-border distribution nature. Thus, subscription into Luxembourg-based funds is often performed through intermediaries acting on behalf of their own customers in other countries.

193. Consequently, the supervisory approach of the CSSF has been tailored to take into account this operational reality and it requires the investment funds, their Investment Fund Managers, or where applicable, any proxy, to perform AML/CFT enhanced due diligence on those intermediaries.

194. The AML/CFT supervisory approach of the CSSF takes into account the roles and responsibilities of the several parties involved in the investment fund industry. The supervisory life cycle starts with AML/CFT controls performed at licensing, continuing on an ongoing basis through off-site and on-site supervisory actions. For instance, dedicated on-site inspections are performed at the level of the Investment Fund Managers as they often decide on the channels and countries of distribution of the funds. These on-site inspections are complemented by supervisory actions on-site and off-site at the level of Luxembourg service providers such as at registrar and transfer agents and at the custodian/depositary bank of the funds.

195. The CSSF's AML/CFT Risk Based Supervisory ("RBS") approach to the sector is subject to a continuous improvement. Lastly, through the addition of two new components. First, an Automatic Score, calculated from a dedicated AML/CFT online questionnaire filled in by investment fund managers, registrar and transfer agents and depositary banks. Second, through an internal Expert Judgement Score. The combination of both sources aims at providing a final score, taking into account several risk criteria and respective mitigation measures implemented by the obliged entities. The RBS is a dynamic process in that the score of an entity may be changed at any point of time, if affected by new information or trigger events. This enables the CSSF to adapt its supervisory actions to emerging threats.

196. Furthermore, the CSSF maintains a database of main findings identified during its AML/CFT onsite inspections and shares them with the private sector on an anonymous basis through its annual reports. Other interactions with the private sector take place notably via regular meetings with obliged entities, events with professional associations, and the publication of AML/CFT guidance through CSSF circulars. In addition, the CSSF makes contact with other competent authorities within Luxembourg and abroad in order to discuss AML/CFT matters and to exchange information through Memoranda of Understanding.

Mexico

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

197. 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.

198. 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.

199. 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 STRs, obtaining at the end the residual risk for each entity.

200. 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.

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

202. 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.

USA

203. The SEC conducts examinations of SEC registrants using a risk‐based approach. A firm may be selected for examination for any number of reasons including, but not limited to, a tip, referral, or complaint; the firm's risk profile; or in connection with a review of a particular compliance risk area. The reason why firms have been selected for examination is non-public information, and typically will not be shared with the firm under examination. ML risks, among others, may be considered in developing a firm's risk profile and the scope of each examination.

204. During examinations, SEC examiners seek to determine whether the entity being examined is, among other things, conducting its activities in accordance with the federal securities laws and the rules thereunder, the bank secrecy act as applicable and the rules of self-regulatory organizations (SRO).

205. Over the past several years, the SEC exam group has recruited industry experts to enhance the national examination program's technology and data analytics and thus advance its risk-based examination approach. The examination staff is increasingly incorporating into its AML reviews such enhanced technology and tools to review vast amounts of data so that the staff can identify suspicious activity from the source trade data rather than relying on the broker-dealer's surveillance reports. The staff can compare the activity it identifies to activity identified by the firm, to test

for weaknesses in a firm's monitoring and reporting of suspicious activity, including assessing the reasonableness of the parameters set by firm. Thus, rather than a simple verification of an AML program's existence, examiners can perform nuanced assessments of the quality of the program.

206. FINRA, the SRO for US broker-dealers, has supervisory duties over approximately 3 700 brokerage firms and 6 29 000 registered securities representatives and conducts the majority of broker-dealer AML examinations. FINRA also examines its member firms on a routine basis for compliance with its rules (including its own AML rule) and the federal securities laws, related to both sales practices and financial operations in its Firm Examination Program. The Firm Examination Program is risk-based, and the frequency of an examination of a member firm is determined through a risk assessment. Thus, a member firm may be examined pursuant to a one or four-year cycle, with higher risk and higher impact firms being examined each year, with a frequency no less than every four years for all firms. AML may be considered for inclusion based on an assessment of risk at that particular firm. When AML is selected for review on a Firm Examination, reviews for particular areas of AML compliance can be narrowly or broadly focused, depending on the specific risks posed by the firm.

207. Firms also may be examined for compliance with certain AML rules and regulations through a Cause Examination or as part of a Sweep Examination, which may encompass multiple firms. Cause Examinations are initiated through terminations for cause, tips, referrals from other regulatory agencies, complaints or by identifying high-risk activity through data analysis. Ongoing risk monitoring is conducted on all FINRA member firms, which includes reviews for compliance with AML-related rules and regulations.

208. In addition, in 2013, FINRA established an AML Investigative Unit to conduct examinations where highly complex or novel money-laundering and AML compliance program concerns exist. In addition to conducting examinations, these AML regulatory specialists provide technical assistance to other examiners and constantly pursue an expansion of knowledge and professional development in the AML arena. The AML Investigative Unit also provides training and education to FINRA staff members and members of the brokerage industry. FINRA has found that this approach leads to better-informed examiners and higher-quality exams.

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; each element may not be relevant in all countries, for all securities providers, for different customer relationships (retail vs. institutional), or for all business activities described in this document.

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 absent any commercial rationale or related corporate action event.
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 absent any commercial rationale or related corporate action event.
2. A transaction pattern indicating a value of transactions just beneath any applicable reporting threshold.
3. Unclear or complex distribution channels that might limit the ability of the investment fund or asset management company to monitor the transactions (e.g. use of a large number of sub-distributors for distributions in third countries)

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 CDD 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 address of the customer, bank or financial institution 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 or requests an inordinate amount of secrecy around a transaction.
14. Customer exhibits unusual concern with the firm's compliance with government reporting requirements, the firm's systems or the firm's AML/CFT policies and controls.
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[33] or correspondent accounts held by the financial intermediary instead of its own accounts.
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.
22. Frequent change of bank account details or information for redemption proceeds, in particular when followed by redemption requests.
23. The usage of brokerage accounts as long term depository accounts for funds.

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

GUIDANCE FOR A RISK-BASED APPROACH
SECURTIES SECTOR

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.

This Guidance focuses on RBA for the securities sector and includes an annex on suspicious activity indicators in relation to the securities sector. 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 FATF Report: Money Laundering and Terrorist Financing in the Securities Sector (October 2009), which outlines vulnerabilities in the sector.

www.fatf-gafi.org | October 2018