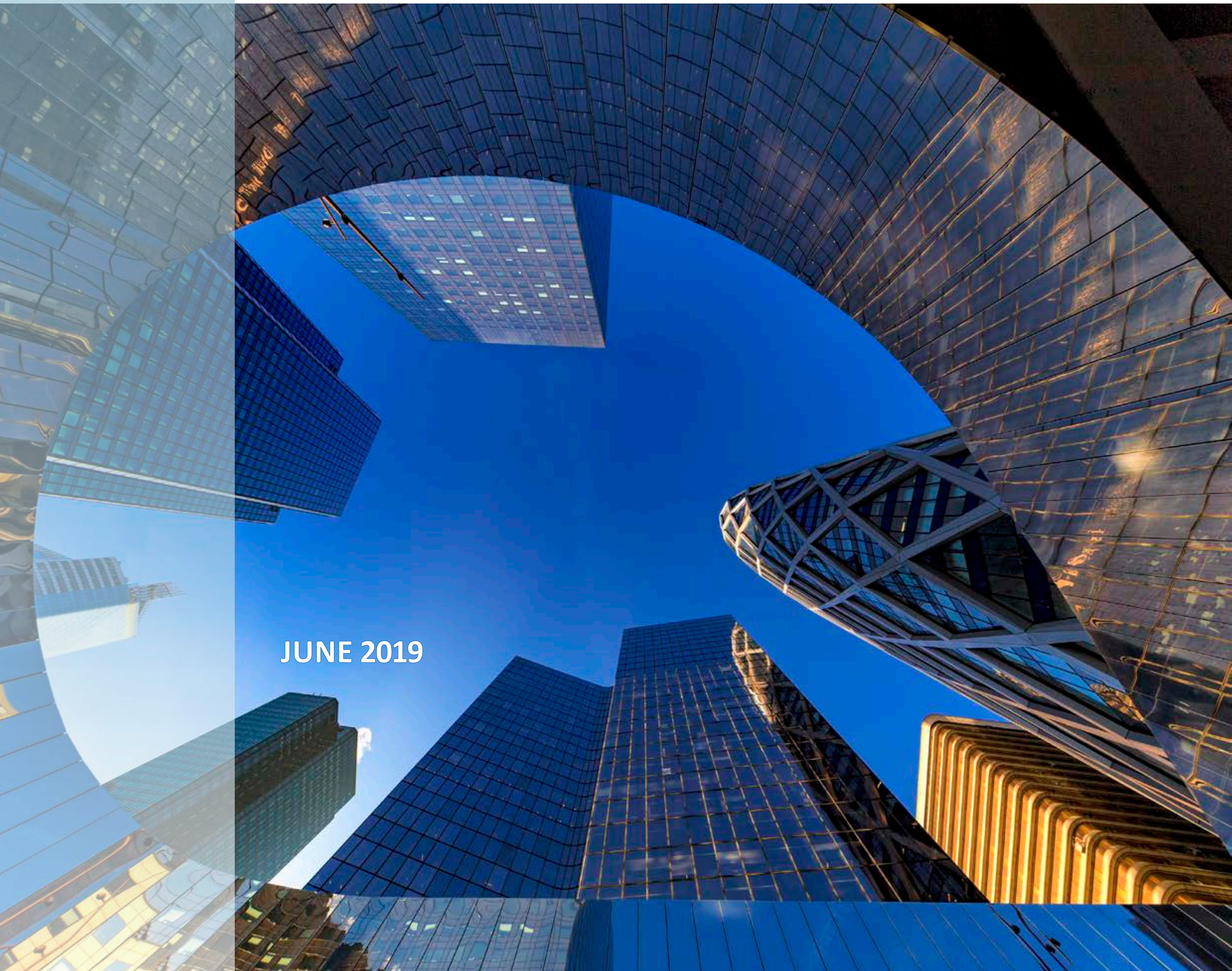
FATF

GUIDANCE FOR A RISK-BASED APPROACH

TRUST AND COMPANY SERVICE PROVIDERS



JUNE 2019

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 (2019), *Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs),* FATF, Paris,
www.fatf-gafi.org/publications/documents/rba-trust-company-service-providers.html

TABLE OF CONTENT

Table of acronyms

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Client[1] due diligence
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
ML	Money laundering
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-based approach
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and company service providers
TF	Terrorist financing

1 In some jurisdictions or professions, the term "customer" is used, which has the same meaning as "client" for the purposes of this document

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 trust and company service providers (TCSPs) 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 the TCSP sector and for their supervisors. The Guidance was developed in partnership with the profession, to make sure it reflects expertise and good practices from within the industry.

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

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

5. The Guidance highlights that TCSPs should design their policies and procedures so that the level of initial and ongoing client due diligence measures addresses the ML/TF risks they are exposed to. In this regard, the Guidance explains the obligations for TCSPs regarding identification and verification of beneficial ownership information and provides examples of standard, simplified and enhanced CDD measures based on ML/TF risk.

6. The Guidance has a section for supervisors of the TCSP sector and highlights the role of self-regulatory bodies (SRBs) in supervising and monitoring. It explains the risk-based approach to supervision as well as supervision of the risk-based approach by providing specific guidance on licensing or registration requirements for the TCSP sector, mechanisms for on-site and off-site supervision, enforcement, guidance, training and value of information-exchange between the public and private sector.

7. The Guidance also highlights the importance of supervision of beneficial ownership requirements and nominee arrangements. It underscores how supervisory frameworks can help ascertain whether accurate and up-to-date beneficial ownership information on legal persons and legal arrangements is maintained by TCSPs and made available in a timely manner to competent authorities when required.

Section I- Introduction and Key Concepts

This Guidance should be read in conjunction with the following, which are available on the FATF website: www.fatf-gafi.org:

a) The FATF Recommendations, especially Recommendations 1, 10, 11, 12, 17, 19, 20, 21, 22, 23, 24, 25 and 28 and their Interpretive Notes (INR), and the Glossary.

b) Other relevant FATF Guidance documents such as:

- The FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)
- FATF Guidance on the Risk-Based Approach for Accountants
- FATF Guidance on the Risk-Based Approach for Legal Professionals
- FATF Guidance on Transparency and Beneficial Ownership (October 2014)

c) Other relevant FATF Reports such as:

- Money Laundering Using Trust and Company Service Providers (October 2010)
- The Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership (July 2018)

Background and context

8. 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]. The FATF has reviewed its 2009 RBA Guidance for trust and company service providers (TCSPs), in order to bring it in line with the new FATF requirements[3] and to reflect the experience gained by public authorities and the private sector over the years in applying the RBA. This revised version applies to the TCSP sector[4] as well as, accountant and legal professionals who provide TCSP services, and financial institutions who are engaged in TCSP activity (e.g. through subsidiaries that conduct TCSP activity).

9. Reference in this Guidance to TCSPs refers to trust and company service providers acting in the course of a business.

10. The RBA Guidance for the TCSP sector was drafted by a project group comprising FATF members, FATF observer member - the Group of International Finance Centre Supervisors and representatives of the private sector. The project group was co-led by the UK, the United States, the Institute of Chartered Accountants in England and Wales, the International Bar Association and the Society of Trust and Estate Practitioners. Membership of the project group is set out in Annex 4.

---

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

3 These services are included in the FATF Glossary under "Designated non-financial businesses and professions at (f)

4 Including both legal and natural persons, see definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary

11. The FATF adopted this updated RBA Guidance for TCSP at its June 2019 Plenary.

Purpose of the Guidance

12. The purpose of this Guidance is to:

a) Support a common understanding of a RBA for TCSPs, financial institutions and designated non-financial businesses and professions (DNFBPs)[5] that maintain relationships with TCSPs, competent authorities and self-regulatory bodies (SRBs)[6] responsible for monitoring the compliance of TCSPs with their AML/CFT obligations;

b) Assist countries, competent authorities and TCSPs in the design and implementation of a RBA to AML/CFT by providing guidelines and examples of current practice, with a particular focus on providing advice to small firms;

c) Recognise the difference in the RBA for different TCSPs who are establishing trusts, companies or other legal entities for the benefit of clients or who are acting as trustees or directors (or providing persons to act as trustees or directors) of such trusts, companies or other legal entities as against TCSPs who are providing more limited services (e.g. registered office services);

d) Outline the key elements involved in applying a RBA to AML/CFT related to TCSPs;

e) Assist financial institutions and DNFBPs that have TCSPs as customers in their role as directors or trustees of a legal person or legal arrangement customer of the financial institution or DNFBP, in identifying, assessing and managing the ML/TF risk associated with TCSPs and their services;

f) Assist countries, competent authorities and SRBs in the implementation of the FATF Recommendations with respect to TCSPs, particularly Recommendations 22, 23 and 28;

g) Assist countries, SRBs and the private sector to meet the requirements expected of them, particularly under IO.3 and IO.4;

h) Support the effective implementation of action plans of NRAs conducted by countries; and

i) Support the effective implementation and supervision by countries of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

Target audience, status and content of the Guidance

13. This Guidance is aimed at the following audience:

a) Practitioners in the TCSP sector;

---

5 See definition of the term 'Designated Non-Financial Businesses and Professions' in the FATF Glossary

6 See definition of the term 'Self-regulatory body' in the FATF Glossary

b) Countries and their competent authorities, including AML/CFT supervisors of TCSPs, SRBs, AML/CFT supervisors of banks and other financial institutions that have TCSPs as customers, and Financial Intelligence Units (FIU); and

c) Practitioners in the banking sector and other financial services sectors and DNFBPs that have TCSPs as customers.

14. The Guidance consists of four sections. Section I sets out introduction and the key concepts. Section II contains key elements of the RBA and should be read in conjunction with specific Guidance to TCSPs (Section III) and guidance to supervisors of TCSPs on the effective implementation of a RBA (Section IV). There are four annexes:

a) Beneficial ownership information in relation to a company, trust or other legal arrangements to whom a TCSP provides services (Annex 1);

b) Glossary of Terminology (Annex 2);

c) Supervisory practices for implementation of the RBA (Annex 3); and

d) Members of the RBA Drafting Group (Annex 4).

15. This Guidance recognises that an effective RBA will take account of the national context, consider the legal and regulatory approach and relevant sector guidance in each country, and reflect the nature, diversity, maturity and risk profile of a country's TCSP sector and the risk profile of individual TCSPs operating in the sector. The Guidance sets out different elements that countries and TCSPs could consider when designing and implementing an effective RBA.

16. This Guidance is non-binding and does not overrule the purview of national authorities[7], including on their local assessment and categorisation of the TCSP sector based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector to assist competent authorities and TCSPs to implement applicable FATF Recommendations effectively. National authorities may take this Guidance into account while drawing up their own Guidance for the sector. DNFBPs should also refer to relevant legislation and sector guidance for the country in which a TCSP customer is based.

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

Terminology

17. Under the FATF definition, Trust and Company Service Providers refers to all persons[8] or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons;

[7] National authorities should however take the Guidance into account when carrying out their supervisory functions.

[8] Including both legal and natural persons, see definition for Designated Non-Financial Businesses and Professions in the FATF Glossary

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

18. The FATF definition of TCSP relates to providers of trust and company services that are not covered elsewhere by the FATF Recommendations, and therefore excludes financial institutions, lawyers, notaries, other independent legal professionals and accountants. Separate guidance has been issued for those sectors, and they should therefore apply that guidance when providing services covered by R.22. However, all those professions/entities engaged in TCSP activities should also refer to the TCSPs guidance, as it is more specifically tailored to TCSP services.

Key features

19. TCSPs can take different forms. In some countries, they may be predominantly legal professionals and accountants. In other countries – particularly in countries with a high concentration of non-resident business – TCSPs are independent trust companies which may be owned and operated by their directors/senior managers, or trust companies that are subsidiaries of financial institutions and DNFBPs. In some cases, these may form part of international non-bank financial groups which provide TCSP services from more than one jurisdiction, or who may be other professionals. In other countries, trust service providers (e.g. trust companies) and company service providers are separate and distinct categories of entities subject to separate regulatory requirements. As a result, not all persons and businesses active in the TCSP industries provide all of the services listed in the definition of a TCSP. Accordingly, risk should be identified and managed on a service-by-service basis.

20. The roles and therefore risks of the different DNFBP constituents, including TCSPs frequently differ. However, in some areas, there are inter-relationships between different DNFBP sectors, and between the DNFBPs and financial institutions. For example, in addition to specialised trust and company service providers, financial institutions, legal professionals, and accountants may also undertake the trust and company services covered by the FATF Recommendations.

Activities carried out by TCSPs

21. TCSPs provide a range of services and activities that differ vastly, e.g. in their methods of delivery, in the depth and duration of the relationships formed with customers, and the size of the operation. For example, some of these entities are single person operations. This Guidance is intended for all TCSPs and sets out a risk-based approach to ensure compliance with FATF's Recommendations.

Vulnerabilities of TCSP services

22. Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trusts and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies[9], which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies[10] formed by TCSPs by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

23. Many aspects of this guidance on applying a RBA to AML/CFT may also apply in the context of predicate offences, particularly for other financial crimes such as tax crimes. The ability to apply the RBA effectively to relevant predicate offences will also reinforce the AML/CFT obligations. TCSPs may also have specific obligations in respect of identifying risks of predicate offences such as tax crimes, and supervisors may have a role to play in oversight and enforcement against those crimes. Therefore, in addition to this guidance, TCSPs and supervisors should have regard to other sources of guidance that may be relevant in managing the risks of predicate offences.

FATF Recommendations applicable to TCSPs

24. The basic intent behind the FATF Recommendations as it relates to TCSPs is to ensure that their operations and services are not abused for facilitating criminal activities and ML/TF. The requirements of R.22 regarding CDD, record-keeping, PEPs, new technologies and reliance on third parties set out in R.10, 11, 12, 15 and 17 should apply to TCSPs in certain circumstances.

25. R.22 applies to TCSPs when they prepare for or carry out transactions for a client concerning the activities set out in paragraph 17 above.

26. R.23 requires that R.18, 19, 20 and 21 should apply to TCSPs when on behalf of or for a client, they engage in a transaction in relation to the activities described to in R.22 above. These Recommendations relate to internal AML/CFT controls, measures to be taken for countries that do not or insufficiently comply with the FATF Recommendations, reporting of suspicious activity and associated prohibitions on tipping off and confidentiality provisions. Section III provides further guidance on the application of R.22 and R.23 obligations to TCSPs.

---

9 A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

10 A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

27. Countries should establish the most appropriate regulatory regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for TCSPs.

Section II – The RBA to AML/CFT

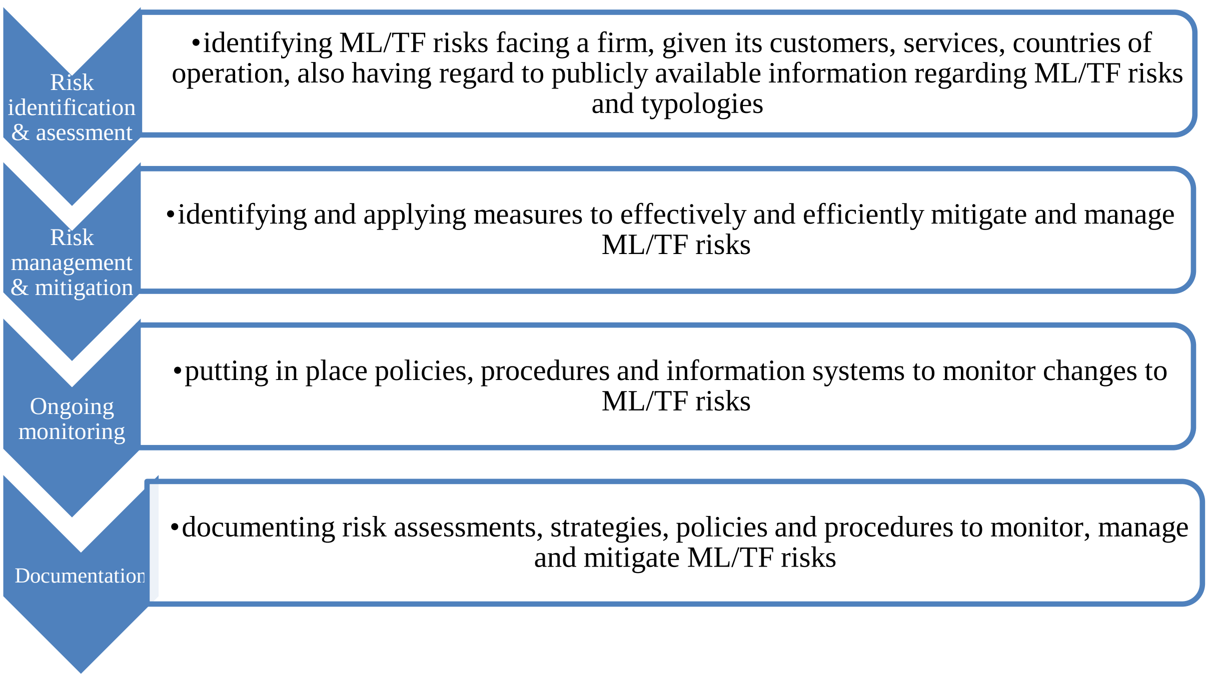
What is the risk-based approach?

28. The RBA to AML/CFT means that countries, competent authorities and DNFBPs, which include TCSPs should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

29. For TCSPs, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, jurisdictions in which they operate and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision, and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

30. The RBA is not a "zero failure" approach; there may be occasions where a TCSP has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that TCSPs must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

31. Key elements of a RBA can be summarised as follows:



The rationale for the RBA

32. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

33. There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.[11]

34. The RBA allows countries, within the framework of the FATF Standards, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are commensurate with the nature of risks.

35. The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and TCSPs.[12]

Application of the risk-based approach

36. The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF. The overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of factors including services, products, customers, geography, preventive measures and the strength of an entity's compliance program.

37. R.1 sets out the scope of application of the RBA as follows:

a) Who 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[13], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[14]

---

11 R.1.

12 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 into account the risks and the flexibility allowed by the RBA, when determining whether there are deficiencies in a country's AML/CFT measures, and their importance *(FATF, 2013f).*

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

14 See INR.1.

b) How should those subject to the AML/CFT regime be supervised or monitored for compliance with this regime? Supervisors should ensure that TCSPs are implementing their obligations under R.1. AML/CFT supervisors should consider a TCSP's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA.

c) How should those subject to the AML/CFT regime be required to comply? The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. TCSPs are required to apply each of the CDD measures under (a) to (d) below[15]: (a) identification and verification of the client's identity; (b) identification and taking reasonable measures to verify the identity of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner; (c) understanding the purpose and nature of the business relationship; and (d) on-going due diligence on the relationship. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

d) Consideration of the engagement in client relationships: TCSPs are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all TCSPs and all their clients or services pose a higher risk when taking account of the risk mitigating measures that have been put in place.

e) Importance of TCSPs to the overall economy: TCSPs often play significant roles in the legal and economic life of a country. The role of TCSPs in supporting the business registration process, finalising documentation for that and providing professional advice is vital. The risks associated with any type of client group is not static and the expectation is that within a client group, based on a variety of factors, individual clients could also be classified into risk categories, such as low, medium-low, medium high or high risk (see section III below for a detailed description). Measures to mitigate risk should be applied accordingly.

Challenges

38. Implementing a RBA can present a number of challenges for TCSPs in identifying what necessary measures they need to take. A RBA requires resources and expertise, both at a country and institutional level, to gather and interpret information on risks, to develop and maintain effective procedures and systems, and to train personnel. A RBA is also reliant on individuals exercising sound and well-trained judgement when designing and implementing procedures and systems. It will also lead to a diversity in practice, although this can result in innovative solutions to address areas of higher risk. On the other hand, TCSPs may be uncertain as to how to comply with the regulatory framework itself and the TCSP sector may find it difficult to apply a uniform approach.

15 See R.10

39. TCSPs need to have a good understanding of the risks and should be able to exercise sound judgement. This requires the profession, and the individuals within it, to build expertise through experience and training. If a TCSP attempts to adopt a RBA without sufficient expertise or understanding and knowledge of the risks faced by the sector, they may make flawed judgements. TCSPs may over-estimate risk, which could lead to wasteful use of resources, or they may under-estimate risk, and therefore deploy insufficient resources, thereby creating vulnerabilities.

40. TCSPs may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. It may also encourage a 'tick-box' approach to risk assessment.

41. Developing sound judgement is reliant on good information and intelligence sharing by designated competent authorities and SRBs. The existence of good practice guidance, training, industry studies and other available information and materials will also assist the TCSPs to make sound risk-based judgements. TCSPs must be able to access this information and guidance easily so that they have the best possible knowledge on which to base their judgements.

42. The services and products TCSPs provide to their clients vary and are not wholly of a financial nature. The FATF Recommendations apply equally to TCSPs when they are engaged in a specified activity, including obligations related to CDD, reporting of suspicious transactions and associated prohibitions on tipping-off, record-keeping, identification and risk management related to politically exposed persons or new technologies, and reliance on other third-party financial institutions and DNFBPs.

Box 1. Particular RBA Challenges for TCSPs

Culture of compliance and adequate resources. Implementing a RBA requires that TCSPs have a sound understanding of the risks and are able to exercise sound judgement. Above all, TCSP and their management should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organisation. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making. The process will benefit from information sharing by relevant competent authorities and SRBs. The provision of good practice guidance by competent authorities and SRBs is also valuable.

S***ignificant variation in services and clients.*** TCSPs may vary substantially in the breadth and nature of services provided and the clients they serve, as well as the size, focus, ownership profile and sophistication of the firm and its employees. In implementing the RBA, TCSPs should make reasonable judgements for their particular services and activities. This may mean that no two TCSPs are likely to adopt the same detailed practices.

Appropriate mitigation measures will also depend on the nature and risks arising from the service provider's role and involvement. Circumstances may vary considerably between providers who represent clients directly as trustees or directors controlling the affairs of the legal arrangement or legal person to those that are engaged for distinct purposes such as provision of registered office only services and who have to rely on information on the company's activities from external directors.

Transparency of beneficial ownership on legal persons and arrangements. TCSPs are involved in the formation, management, or administration of legal entities and arrangements, though in many countries any legal or natural person also may be able to conduct these activities. Where TCSPs do play this "gatekeeper" role, they may be challenged in obtaining and keeping current and accurate beneficial ownership information depending upon the nature and activities of their clientele. Other challenges may arise when on-boarding new clients with minimal economic activity associated with the legal entity and/or its owners, controlling persons, or beneficial owners, established in another jurisdiction. Finally, whether the source of beneficial ownership information is a public registry, another third party source, or the client, there is always potential risk in the correctness of the information, in particular where the underlying information has been self-reported. Those risks notwithstanding, the start point in determining beneficial ownership should almost always start with questions to the immediate client, having determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the client is a publicly listed company. The information provided by the client should then be appropriately confirmed by reference to public registers and other third party sources where possible. This may require further and clarifying questions to be put to the immediate client. The goal is to ensure that the TCSP is reasonably satisfied about the identity of the beneficial owner. For more practical guidance on beneficial ownership, refer to the guidance in Box 2.

Risk of criminality. TCSPs should be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may commit or become an accessory to the commission of a substantive offence of ML/TF. TCSPs must protect themselves from misuse by criminals and terrorists. This includes the sources and methods used for providing payments for the TCSP's services, which may dictate greater focus on monitoring of clients and their funds for unusual or suspicious activity.

Allocating responsibility under a RBA

43. 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. TCSPs should identify and assess their own ML/TF risk taking account of

the NRAs in line with R.1 as well as the national legal and regulatory framework, including any areas of prescribed significant risk and mitigation measures. TCSPs are required to take appropriate steps to identify and assess their ML/TF risks and have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.[16] Where ML/TF risks are higher, TCSPs should always apply enhanced due diligence, although national law or regulation might not prescribe exactly how these higher risks are to be mitigated (e.g. varying the degree of enhanced ongoing monitoring).

44. Strategies adopted by TCSPs to mitigate ML/TF risks has to take account of the applicable national legal, regulatory and supervisory frameworks. When determining the extent to which TCSPs can decide how to mitigate risk, countries should consider the ability of the sector to effectively identify and manage ML/TF risks as well as the expertise and resources of their supervisors to adequately supervise how TCSPs manage ML/TF risks and take action to address any failures. Countries may also consider evidence from competent authorities on the level of compliance in the sector, and the sector's approach to dealing with ML/TF risk. Countries whose services sectors are emerging or whose legal, regulatory and supervisory frameworks are still developing, may determine that TCSPs are not fully equipped to effectively identify and manage ML/TF risk. In such cases, a more prescriptive implementation of the AML/CFT requirements may be appropriate until understanding and experience of the sector is strengthened.[17]

45. TCSPs should not be exempted from AML/CFT supervision even where their compliance controls are adequate. However, the RBA allows competent authorities to focus more supervisory resource on higher risk entities.

Identifying ML/TF risk

46. Access to accurate, timely and objective information on 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, SRBs, financial institutions and TCSPs. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to share important information on ML/TF risks and threats, or where access to information is restricted by censorship, it will be difficult for TCSPs to correctly identify ML/TF risk.

47. R.34 requires competent authorities, supervisors and SRBs to establish guidelines and provide feedback to financial institutions and DNFBPs. Such guidelines and feedback help institutions and businesses to identify the ML/TF risks and to adjust their risk mitigating programmes accordingly.

Assessing ML/TF risk

48. Assessing ML/TF risk requires countries, competent authorities, including supervisors, SRBs and TCSPs 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 impact that these would have, on the individual TCSP, the entire sector and on the national economy. As a starting step,

16 R.1 and INR.1.

17 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.

ML/TF risks are often classified as low, medium-low, medium, medium-high and high. Assessing ML/TF risk therefore goes beyond the mere gathering of quantitative and qualitative information, without its proper analysis; this information forms the basis for effective ML/TF risk mitigation and should be kept up-to-date to remain relevant.[18]

49. Competent authorities, including supervisors and SRBs should employ skilled and trusted personnel, recruited through fit and proper tests, where appropriate. They should be technically equipped commensurate with the complexity of their responsibilities. TCSPs that are required to routinely conduct a high volume of enquiries when on-boarding clients, (e.g. because of the size and geographic footprint of the firm) may also consider engaging skilled and trusted personnel who are appropriately recruited and checked. Such TCSPs are also likely to consider using the various technological options (including artificial intelligence) and software programs that are now available to assist in this regard.

50. TCSPs should develop internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees. TCSPs should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities.

Mitigating and managing ML/TF risk

51. The FATF Recommendations require that, when applying a RBA, DNFBPs, countries, competent authorities and supervisors decide on the most appropriate and effective way to mitigate and manage the ML/TF risks they have identified. They should take enhanced measures to manage and mitigate situations when the ML/TF risk is higher. In lower risk situations, less stringent measures may be applied.[19]

a) Countries may decide not to apply some of the FATF Recommendations requiring TCSPs to take certain actions, provided (i) there is a proven low risk of money laundering and terrorist financing, this occurs in strictly limited and justified circumstances and it relates to a particular type of TCSPs or (ii) a financial activity is carried out by a natural or legal person on an occasional or very limited basis such that there is a low risk of ML/TF, according to the exemptions of INR 1.6 are met.

b) Countries looking to apply simplified measures should conduct an assessment to ascertain the lower risk connected to the category of customers and clients or products targeted, establish the lower level of the risks involved, and define the extent and the intensity of the required AML/CFT measures, provided that the specific conditions required for one of the exemptions of INR 1.6 are met. Specific Recommendations set out in more detail how this general principle applies to particular requirements.[20]

18 FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

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

20 For example, R.22 on Customer Due Diligence.

Developing a common understanding of the RBA

52. The effectiveness of a RBA depends on a common understanding by competent authorities and TCSPs of what the RBA entails, how it should be applied and how ML/TF risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, TCSPs should deal with the risks they identify. Competent authorities should issue risk-based approach guidance to TCSPs on meeting their legal and regulatory AML/CFT obligations. Supporting ongoing and effective communication between competent authorities and the sector is essential.

53. Competent authorities should acknowledge that in a risk-based regime, not all TCSPs will adopt identical AML/CFT controls. On the other hand, TCSPs should understand that a RBA does not exempt them from applying effective AML/CFT controls with a RBA.

Section III – Guidance for TCSPs

Risk identification and assessment

54. TCSPs should take appropriate steps to identify and assess the risk firm-wide given their particular client base that they could be used for ML/TF. They should document those assessments, keep these assessments up-to-date and have appropriate mechanisms in place to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

55. ML/TF risks can be organised into three categories: (a) country/geographic risk; (b) client risk, and (c) transaction/service and associated delivery channel risk. The risks and red flags listed in each category are not exhaustive but provide a starting point for TCSPs to use when designing their RBA.

56. TCSPs should also refer to their country's NRAs and risk assessments performed by the competent authorities and supervisors.

57. When assessing risk, TCSPs should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in TCSP services/sector, risk reports in other jurisdictions where the TCSP based in and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions.

58. TCSPs may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profiles are also important. Competent authorities should consider how they can best alert TCSPs to the findings of any national risk assessments, the supranational risk assessments and any other information which may be relevant to assess the risk level particular to a TCSP practice in the relevant country.

59. Due to the nature of services that a TCSP generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most TCSPs. The TCSP's knowledge of the client and its business will develop throughout the duration of a longer term and interactive professional relationship. However, although individual TCSPs are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationship. TCSPs will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g. one-off client relationship). TCSPs should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

60. Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow TCSPs to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the TCSP's role and involvement. Circumstances may vary considerably between TCSPs who represent clients on a single transaction and those involved in a long term relationship.

61. The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. A TCSP may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring TCSP).

62. TCSPs may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling TCSPs, where required, to subject each client to reasonable and proportionate risk assessment.

63. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the TCSP and/or firm. These criteria, however, should be considered holistically and not in isolation. TCSPs, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

64. Although there is no universally accepted set of risk categories, the examples provided in this Guidance are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. carrying out company management services may entail greater risk than other services).

65. Criminals deploy a range of techniques and mechanisms to obscure the beneficial ownership of assets and transactions. Many of the common mechanisms/techniques have been compiled by FATF in the previous studies, including the 2014 FATF Guidance on Transparency and Beneficial Ownership and the 2018 Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership. TCSPs may refer to the studies for more details on the use of obscuring techniques and relevant case studies.

66. A practical starting point for firms (especially smaller firms) and TCSPs (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

a) **Client acceptance and know your client policies:** identify the client (and its beneficial owners) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth of the client[21], its owners and the purpose and nature of the transaction.

[21] The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the

b) **Engagement acceptance policies:** Understand the nature of the work. TCSPs should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where a TCSP does not have the requisite expertise, the TCSP should not undertake the work.

c) **Understand the commercial or personal rationale for the work:** TCSPs need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. TCSPs however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

d) **Be attentive to red flag indicators:** exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity, or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/indicators of suspicion. Then consider what action, if any, needs to be taken.

e) The outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

f) TCSPs should adequately document and record steps taken under a) to e).

Country/Geographic risk

67. The provision of services by a TCSP may be higher risk when features of such services are connected to a higher risk country, for example:

a) the origin, or current location of the source of funds in the trust, company or other legal entity;

b) the country of incorporation or establishment of the company or the trusts;

c) the location of the major operations or assets of the trust, company or other legal entity; and

d) the country in which any of the following is a citizen or tax resident: a settlor, beneficiary, protector or other natural person exercising effective control over the trust or any beneficial owner or natural person exercising effective control over the company or other legal entity.

---

activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

68. There is no universally agreed definition of a higher risk country or geographic area but TCSPs should pay attention to:

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 organised crime, corruption, or other criminal activity, including being a major source or a major transit country 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.

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

e) Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

Client risk

69. In the examples given below, the client of TCSPs may be an individual who is a settlor or beneficiary of a trust, or beneficial owner of a company, or other legal entity that is, for example, trying to obscure the real beneficial owner or natural person exercising effective control of the trust, company or other legal entity. The client may also be a representative of a company's or other legal entity's senior management who are, for example, trying to obscure the ownership structure.

70. The key risk factors that TCSPs should consider are:

a) The TCSP's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.

b) The client include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients (Please refer to the FATF Guidance (2013) on politically-exposed persons for further guidance on how to identify PEPs).

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.

c) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).

d) Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

   i. Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

   ii. Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason.

   iii. Use of trust structures for tax evasion or to obscure ownership in order to place assets out of reach to avoid future liabilities.

e) Unusual complexity in control or ownership structures without a clear explanation, where there are certain transactions, structures, geographical location, international activities or other factors are not consistent with the TCSP's understanding of the client's business or economic purpose behind the establishment or administration of the trust, company or other legal entity with respect to which the TCSPs are providing services.

f) Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such.

g) The offer by the person giving instructions to the TCSP to pay extraordinary fees for services, which would not ordinarily warrant such a premium.

h) The relationship between employee numbers/structure is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets compared to similar businesses)

i) Sudden activity from a previously dormant client without a clear explanation.

j) Clients that start or develop an enterprise with unexpected profile or abnormal business cycles or clients that enter into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

k) Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.

l) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

m) Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).

n) Clients who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons and are otherwise evasive or very difficult to reach, when this would not normally be expected. Subsequent lack of contact, when this would normally be expected.

o) Inexplicable changes in ownership.

p) Activities of the trust, company or other legal entity are unclear or different from the stated purposes under trust deeds or internal regulations of the company or foundation.

q) The legal structure has been altered frequently and/or without adequate explanation (e.g. name changes, transfer of ownership, change of beneficiaries, change of trustee or protector, change of partners, change of directors or officers).

r) Management of any trustee, company or legal entity appears to be acting according to instructions of unknown or inappropriate person(s).

s) Unreasonable choice of TCSP without a clear explanation, given the size, location or specialisation of the TCSP.

t) Frequent or unexplained change of professional adviser(s) or members of management of the trustee, company or other legal entity.

u) The person giving instructions to the TCSP is reluctant to provide all the relevant information or the TCSP has reasonable grounds to suspect that the provided information is incorrect or insufficient.

v) Clients who request that transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for TCSPs to perform a proper risk assessment.

w) Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.

x) Clients with previous convictions for crimes that generated proceeds, who instruct TCSPs (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.

y) Clients who change their means of payment for a transaction at the last minute and without justification (or with suspect justification), or where there is a lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

z) The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

aa) Clients seeking to obtain residents rights or citizenship in the country of establishment of the TCSP in exchange for capital transfers, purchase of property or government bonds, or investment in corporate entities.

Transaction/service and associated delivery channel risk

71. Services which may be provided by TCSPs and which (in some circumstances) risk being used to assist money launderers may include:

a) Use of pooled client accounts or safe custody of client money or assets or bearer shares, without justification.

b) Situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or other legal entities, or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting trustees of such a trust.

d) Services where TCSPs may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.

e) Services that are capable of concealing beneficial ownership from competent authorities.

f) Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants than is normal under the circumstances and in the experience of the TCSP.

g) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

h) Transactions using unusual means of payment (e.g. precious metals or stones).

i) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

j) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

k) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

l) Power of Representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

m) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

n) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.

o) Commercial, private, or real property transactions or services to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons.

p) Products/services that have inherently provided more anonymity or confidentiality without a legitimate purpose.

q) Existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for. These might include:

   i. Over or under invoicing of goods/services.

   ii. Multiple invoicing of the same goods/services.

   iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

   iv. Multiple trading of goods/services.

r) Any attempt by the settlor, trustee, company or other legal entity to enter into any fraudulent transaction.

s) Any attempt by the settlor, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax in any relevant jurisdiction.

Variables that may impact on a RBA and risk

72. While all TCSPs should robust high standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst TCSPs, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating a RBA that also complies with the existing obligations of TCSPs.

73. Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large law firms. TCSPs in many jurisdictions and practices are required to conduct both a risk assessment of the general risks of their practice, and

of all new clients and current clients engaged in one-off specific transactions. The emphasis must be on following a RBA.

74. A significant factor to consider is whether the client and proposed work would be unusual, risky or suspicious for the particular TCSP. This factor must always be considered in the context of the practice of TCSP. The RBA methodology of TCSP may thus take into account risk variables specific to a particular client or type of work. Consistent with the RBA and proportionality, the presence of one or more of these variables may cause a TCSP to conclude that either enhanced CDD and monitoring is warranted, or conversely that standard CDD and monitoring can be reduced, modified or simplified. When reducing, modifying or simplifying CDD, TCSPs should always adhere to the minimum requirements as set out in national legislation These variables may increase or decrease the perceived risk posed by a particular client or type of work and may include:

75. Examples of factors that may increase risk are:

a) Unexplained urgency of assistance required.

b) Unusual sophistication of structure, including complexity of control and governance arrangements and use of multiple TCSPs.

c) The irregularity or limited duration of the client relationship. One-off engagements for the establishment of complex trust, company or other arrangements involving legal entities without ongoing involvement may present higher risk.

76. Examples of factors that may decrease risk are:

a) Involvement of financial institutions or other DNFBPs or TCSPs which are regulated in their home jurisdiction and subject to appropriate AML/CFT regulation.

b) Role or oversight of a regulator or multiple regulators (e.g. regulating TCSPs, trustees or any other person exercising effective control).

c) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk. In addition, a relationship may present less risk where, for example, the TCSP provides an integrated service, including acting as or providing trustees or directors of the trust, company or other legal entity and responsibility for preparation of accounts or maintaining the books and financial records of such trust, company or other legal entity.

d) Trusts, companies or other legal entities that are transparent and well-known in the public domain.

e) Listed entities and other business arrangements, such as pension trusts and employee benefit trusts and other trusts used for commercial purposes.

f) TCSP’s familiarity with a particular country, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

Documentation of risk assessments

77. TCSPs must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement. However, competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.[23]

78. TCSPs may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner is important.

79. Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment, and dated. In assessing the risk profile of the client at this stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

80. A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be made accessible to all professionals having to perform AML/CFT duties.

81. Where TCSPs are involved in longer term transactions, risk assessments should be undertaken at suitable intervals across the life of the transaction, to ensure no significant risk factors have changed in the intervening period (e.g. new parties to the transaction, new sources of funds etc.).

82. A final risk assessment should be undertaken before a transaction has completed, allowing time for any required suspicious activity report, where required and appropriate, to be filed and any authority to move or transfer assets to be obtained from law enforcement (in countries where this is applicable).

Risk mitigation

83. TCSPs should have policies, controls and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls and procedures should be approved by senior management and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and supervisors. Measures and controls may include:

a) General training on ML/TF methods and risks relevant to TCSPs.

b) Targeted training for increased awareness by the TCSPs providing specified activities to higher risk clients or to TCSPs undertaking higher risk work.

---

23 Paragraph 8 of INR.1.

c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.

d) Periodic review of the services offered by the TCSP, and the periodic evaluation of the AML/CFT framework applicable to the TCSP and the TCSP's own AML/CFT procedures, to determine whether the ML/TF risk has increased and adequate controls are in place to mitigate those increased risks.

e) Reviewing client relationships on a periodic basis to determine whether the ML/TF risk has increased.

Initial and ongoing CDD (R.10 and 22)

84. TCSPs should design CDD procedures to enable them to form a reasonable certainty that they know the true identity of the relevant beneficial owners of, or natural persons who actually exercise effective control over, the trust, company or other legal entity and, with an appropriate degree of confidence, know the true purpose behind the establishment or use of the trust, company or other legal entity. TCSPs' procedures should include procedures:

a) For identifying the client and verifying that client's identity using reliable, independent source documents, data or information.

b) For identifying the relevant beneficial owners and natural persons who actually exercise control as set out in Annex 1 and taking reasonable measures to verify the identity of such persons (i.e. on a risk-based approach). This is articulated in the following box:

Box 2. Beneficial ownership information obligations
(see R.10, R.22 and INR.10)

R.10 sets out the instances where TCSPs will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. TCSPs should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. TCSPs should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.8-10.12.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. TCSPs can verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. TCSPs can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the TCSP is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client, and may include conducting public searches as well as by seeking information directly from the client. TCSPs will likely need to obtain the following information for a client that is a legal entity:

a) the name of the company;
b) the company registration number;
c) the registered address and/ or principal place of business (if different);
d) the identity of shareholders and their percentage ownership;
e) names of the board of directors or senior individuals responsible for the company's operations; and
f) the law to which the company is subject and its constitution; and
g) the types of activities and transactions in which the company engages.

To verify the information listed above, TCSPs may use sources such as the following:

a) constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
b) details from company registers; and
c) shareholder agreements or other agreements between shareholders concerning control of the legal person;
d) filed audited accounts.

TCSPs should adopt a RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to-date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

c) Enabling the TCSP to understand and, as appropriate, obtain information on the purpose and intended purpose of the trust, company or other legal entity.

d) Conducting ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to respond to requests for information from an FIU and the law enforcement agencies.

85. Where risks are higher, TCSPs should obtain information about the source of funds in the trust, company or other legal entity and source of wealth in relation to the settlor or beneficial owner.

86. TCSPs should design their policies and procedures so that the level of CDD addresses the risk of the trust, company or other legal entity with respect to which services are being provided by the TCSP being used for ML/TF. TCSPs should design a standard level of CDD for normal risk clients and a reduced or simplified CDD process for low risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that the TCSP has assessed as high risk. These activities may be carried out in conjunction with the TCSP's normal acceptance procedures, and will take into account any specific jurisdictional requirements for CDD in relation to the trust, company or other legal entity and any trustee, settlor, protector, beneficial owner or other natural person exercising effecting control over the trust, company or other legal entity.

87. In the normal course of their work, TCSPs are likely to learn more about some aspects of the trust, company or other legal entity, and the trustee, settlor, protector, beneficial owners or other natural persons exercising effective control, than other advisors. This information is likely to help the TCSP dynamically assess the ML/TF risk.

88. Identification of, company or other legal entity, any trustee or of any settlor, beneficial owner or natural person exercising effective control should be periodically reviewed. This is to ensure that changes in ownership or control are properly recorded. This may be carried out in conjunction with any professional requirements for client continuation processes.

89. Public information sources may assist with this ongoing review. The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominee shareholders and complex structures.

90. The following box provides a non-exhaustive list of examples of standard, enhanced and simplified CDD:

Box 3. Examples of Standard/Simplified/Enhanced CDD measures (see also INR.10)

Standard CDD

- Identifying the client and verifying that client's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the TCSP is satisfied about the identity of beneficial owner. For legal persons and arrangements, this should include understanding the ownership and control structure of the client and gaining an understanding of the client's source of wealth and source of funds, where required

- Understanding and obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the business and risk profile the client, including, where necessary, the source of wealth and funds

Simplified CDD

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client'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
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

Enhanced CDD

- Obtaining additional information on the trustee, settlor, beneficial owner or natural person exercising effective control of the trust, company or other legal entity (as described in Annex 1) (e.g. occupation, overall wealth, information available through public databases, internet), and updating more regularly the identification data of such persons and sources which can be regarded as credible
- Obtaining information on the reasons for intended or performed transactions carried out by the trust, company or other legal entity administered by the TCSP
- Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the settlor (as described in Annex 1) and evidencing this through appropriate documentation obtained
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the TCSPs policies should enable it to disregard source documents, data or information which is perceived to be unreliable)
- Considering 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. This could include obtaining appropriate documentation concerning the source of wealth or funds
- Increasing the frequency and intensity of transaction monitoring
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

- Where appropriate, requiring the first payment to be carried out through an account in the name of the trust, company or other legal entity with a bank subject to similar CDD standards
- Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of engagement teams responsible for the client
- Enhanced CDD may also include lowering the threshold of ownership (e.g. below 25%), to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Politically exposed persons (PEP) (R.12)

91. TCSPs should take reasonable measures to identify any trustee, settlor, beneficial owner or natural person exercising effective control (as further described in Annex 1) in relation to a trust, company or other legal persons whether they are a PEP or a family member or close associate of a PEP. If the client or beneficial owner is a PEP or a family member or close associate of a PEP, TCSPs should perform the following additional procedures:

a) obtain senior management approval for establishing (or continuing, for existing structures) such business relationships;

b) take reasonable measures to establish the source of wealth and source of funds in relation to the settlor, beneficiaries who receive distributions, or natural persons exercising effective control over a trust or beneficial owners or natural persons exercising effective control over a legal entity or other arrangement identified as PEPs (as described in Annex 1); and

c) conduct enhanced ongoing monitoring of the business relationship.

92. Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, whether the PEP has access to official funds, the PEP's home country, the type of work the PEP is instructing the TCSP to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP's home country.

93. The nature of the risk should be considered in light of all relevant circumstances, such as:

a) The nature of the relationship between the client and the PEP. If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) The nature of the client (e.g. where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

c) The nature of the services sought. For example, lower risks may exist where a PEP is not the client but a director of a client that is a public listed company or regulated entity and the client is purchasing property for adequate consideration.

Ongoing monitoring of clients and specified activities (R.10 and 22)

94. TCSPs are not expected to scrutinise every transaction carried out by a trust, company or other legal entity to whom the TCSP provides services. Some services are provided only on a one-off basis, without a continuing relationship with the trust, company or other legal entity and without the TCSP having access to the books and records of the trust, company or other legal entity and/or bank records. However, many of the professional services provided by TCSPs enable them to identify suspicious activity or transactions carried out using trust, companies or other legal entities. For example, their direct knowledge of, and access, to the records and management processes and operations of such structures as well as through close working relationships with trustees, settlors, managers and beneficial owners may help TCSPs make a determination in this regard. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements and corporate filings) would also enable the relevant TCSPs to develop a better understanding of the activities of their clients.

95. TCSPs need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgement in the formulation of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional TCSPs' functions and relationships.

96. Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that the trustees, settlors, beneficial owners and natural persons exercising effective control (as described in Annex 1) are aware of any changes in the client's identity and risk profile established on acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds and wealth where necessary, to judge consistency with expected behaviour based on CDD information. As discussed below, ongoing monitoring may also give rise to filing a STR.

97. The TCSP should also consider reviewing CDD on an engagement/assignment basis for each trust, company or other legal entity with respect to which the TCSP provides ongoing services. Well-known, reputable, long-standing trustees, settlors, beneficial owners or other natural persons exercising effective control (as described in Annex 1) may suddenly request a new type of service that is not in line with the previous relationship with the TCSP. Such an assignment may suggest a greater level of risk.

98. TCSPs should not conduct investigations into suspected ML/TF on their own but instead file a STR or if the behaviour is egregious they should contact the FIU, law enforcement or supervisors, as appropriate, for guidance. Within the scope of engagement, a TCSP should be mindful of the prohibition on "tipping off" the individual concerned where a suspicion has been formed. Carrying out additional investigations, which are not within the scope of the engagement should also be considered against the risk alerting a money launderer.

99. When deciding whether or not an activity or transaction is suspicious, TCSPs may need to make additional enquiries (within the normal scope of the assignment or business relationship) of the individual or entity concerned or their records – this could typically be done as part of the TCSP's CDD process. Normal commercial enquiries, being made to fulfil duties to the trust, company or other legal entity with respect to which the TCSP provides services, may assist in understanding an activity or transaction to determine whether or not it is suspicious.

Suspicious transaction reporting, tipping-off, internal controls and higher-risk countries (R.23)

100. R.23 sets out obligations for TCSPs on reporting and tipping-off, internal controls and higher-risk countries (R.20, R.21, R.18 and R.19)

Suspicious transaction reporting and tipping-off (R.20, 21 and 23)

101. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must always be made promptly. The requirement to file a STR is not subject to a risk-based approach, but must be made promptly whenever required in the country concerned.

102. TCSPs may be required to report suspicious activities, as well as specific suspicious transactions, and so may make reports on a number of scenarios including suspicious business structures or management profiles which have no legitimate economic rationale. As specified under INR.23, where TCSPs seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

103. However, a RBA is appropriate for identifying a suspicious activity or transaction, by directing additional resources at those areas a TCSP has identified as higher risk. The designated competent authorities or SRBs may provide information to TCSPs, which will be useful to them to inform their approach for identifying suspicious activity or transactions, as part of a RBA. A TCSP should also periodically assess the adequacy of its system for identifying and reporting suspicious activity or transactions.

104. TCSPs should review their existing CDD if they have a suspicion of ML/TF.

Internal controls and compliance (R.18 and 23)

105. In order for TCSPs to have an effective risk-based approach, the risk-based process must be embedded within the internal controls of the firm and they must be appropriate for the size and complexity of the firm.

Internal controls and governance

106. Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

107. The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being

offered. In addition to other compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

a) designating an individual, or individuals, at management level responsible for managing AML/CFT compliance;

b) designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate. These policies and procedures should be implemented across the firm and include:

   – risk-based CDD policies, procedures and processes;

   – ensure that adequate controls are in place before new services are offered; and

   – adequate controls for accepting higher risk clients or providing higher risk services, such as management approval;

c) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;

d) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;

e) providing senior management with a regular report of compliance initiatives, identify compliance deficiencies, corrective action taken, and STRs filed;

f) planning for changes in management, staff or firm structure so that there is compliance continuity;

g) focusing on meeting all regulatory record keeping and reporting requirements, recommendations for AML/CFT compliance and providing for timely updates in response to changes in regulations;

h) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;

i) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;

j) providing for appropriate training to be given to all relevant staff;

k) having appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP or a person subject to applicable financial sanctions;

l) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, escalation to senior management or additional review and/or consultation);

m) providing increased focus on a TCSP's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;

n) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the TCSP operates and the services it provides; and

o) providing for an AML/CFT compliance function and review programme, as appropriate, given the scale of the organisation and the nature of the TCSP's practice.

108. TCSPs should review the firm-wide risk assessment that takes into account the size and nature of the practice; the existence of high-risk clients (if any); and the provision of high-risk services (if any). Once completed, the firm-wide risk assessment will assist the firm in designing its policies and procedures and in establishing the level of resources it will require to manage and mitigate the ML/TF risks.

109. TCSPs should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/CFT processes. As these solutions are likely to become more affordable, and more tailored to the needs of TCSPs as they continue to develop, this may be particularly important for smaller firms that may be less able to commit significant resources of time to these activities.

110. Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole owner/proprietor firms, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

Internal mechanisms to ensure compliance

111. The TCSP (at the senior management level) should monitor effectiveness of its internal controls. If the TCSP identifies any weaknesses in those internal controls, it should design improved procedures.

112. The most effective tool to monitor the internal controls is a regular independent compliance review. A member of staff that has a good working knowledge of the firm's AML/CFT internal control framework, policies and procedures and is sufficiently senior to challenge them should perform the review. The person conducting an independent review should not be the same person who designed or implemented the controls being reviewed. The compliance review should include a review of CDD documentation to confirm that staff are properly applying the firm's procedures.

113. If the compliance review identifies areas of weakness and makes recommendations on how to improve the policies and procedures, then senior management should monitor how the firm is acting on those recommendations.

114. The TCSP should consider its firm-wide risk assessment regularly and make sure that the policies and procedures continue to direct effort to those areas where risk of ML/TF is highest.

Vetting and recruitment

115. TCSPs should consider the skills, knowledge and experience of staff both before they are appointed to their role and on an ongoing basis. The level of assessment should be proportionate to their role in the firm and the ML/TF risks they may encounter. Assessment may include criminal records checking and other forms of pre-employment screening such as credit reference checks and background verification (as permitted under national legislation) for key staff positions.

Education, training and awareness

116. R.18 requires that TCSPs provide their staff with AML/CFT training. For TCSPs, and those in smaller firms in particular, such training may also assist with raising awareness of monitoring obligations. A TCSP's commitment to having appropriate controls in place relies fundamentally on both training and awareness. This requires a firm-wide effort to provide all relevant staff with at least general information on AML/CFT laws, regulations and internal policies.

117. Firms should provide targeted training for increased awareness by the TCSPs providing specified activities to higher-risk clients and to TCSPs undertaking higher-risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted towards the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

118. In line with a RBA, particular attention should be given to risk factors or circumstances occurring in TCSP's own practice. In addition, competent authorities, SRBs and representative bodies should work with educational institutions to ensure that the relevant curricula address ML/TF risks. The same training should also be made available for students taking courses to train to become TCSPs.

119. TCSPs must periodically provide their employees with appropriate AML/CFT training. In ensuring compliance with this requirement, TCSPs may take account of any AML/CFT training included in entry requirements and continuing professional development requirements for their professional staff. They must also ensure appropriate training for any relevant staff without a professional qualification, at a level appropriate to the functions being undertaken by those staff, and the likelihood of their encountering suspicious activities.

120. The overall risk-based approach and the various methods available for training and education gives TCSPs flexibility regarding the frequency, delivery mechanisms and focus of such training. TCSPs should review their own staff and available resources and implement training programs that provide appropriate AML/CFT information that is:

a) tailored to the relevant staff responsibility (e.g. client contact or administration);

b) at the appropriate level of detail (e.g. considering the nature of services provided by the TCSP);

c) at a frequency suitable to the risk level of the type of work undertaken by the TCSP; and

d) used to test to assess staff knowledge of the information provided.

Higher-risk countries (R.19 and 23)

121. Consistent with R.19, TCSPs should apply effective enhanced due diligence measures (also see paragraph 68), proportionate to the risks, to business relationships and transactions with clients from countries for which this is called for by the FATF.

Section IV – Guidance for supervisors

122. A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resource to areas of higher ML/TF risk. R.28 requires that TCSPs are subject to adequate AML/CFT regulation and supervision. While it is each country's responsibility to ensure there is an adequate national framework in place in relation to regulation and supervision of TCSPs, any relevant supervisors and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.[24] The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate with the ML/TF risks identified. This applies to the way supervisory authorities allocate their resources.

The risk-based approach to supervision

Supervisors and SRBs' role in supervision and monitoring

123. According to R.28, countries must ensure that DNFBPs are subject to effective oversight through the supervision performed by a supervisor or by an appropriate SRB, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

124. A SRB is body representing a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and to practise in the profession. A SRB also performs supervisory or monitoring functions (e.g. to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession).

125. Supervisors and SRBs should have adequate powers to perform their supervisory functions (including powers to monitor and to impose effective, proportionate and dissuasive sanctions), and adequate financial, human and technical resources. They should determine the frequency and intensity of their supervisory or monitoring actions on TCSPs on the basis of their understanding of the ML/TF risks, and taking into consideration the characteristics of the TCSPs, in particular their diversity and number.

126. Countries should ensure that supervisors and SRBs are equipped in identifying and sanctioning non-compliance by its members. Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

127. Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population, or represents those people, the relevant person should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

---

24 See INR 28.1.

128. Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas.

Understanding ML/TF risk- the role of countries

129. Countries should ensure, to the extent the national framework allows, that TCSPs apply a RBA that reflects the nature, diversity and maturity of the sector and its risk profile as well the ML/TF risks associated with individual TCSPs.

130. Access to information about ML/TF risks is essential for an effective RBA. Countries are required to take appropriate steps to identify and assess ML/TF risks on an ongoing basis in order to (a) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (b) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (c) make information available for AML/CFT risk assessments conducted by TCSPs and the jurisdiction's national risk assessment. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to competent authorities, SRBs and TCSPs. In situations where some TCSPs have limited capacity to identify ML/TF risks, countries should work with the sector to understand their risks.

131. Supervisors and SRBs should, as applicable, draw on a variety of sources to identify and assess ML/TF risks. These may include, but will not be limited to, the jurisdiction's national risk assessments, supranational risk assessments, domestic or international typologies, supervisory expertise and FIU feedback. The necessary information can also be obtained through appropriate information-sharing and collaboration among AML/CFT supervisors, when there are more than one for different sectors (legal professionals, accountants and TCSPs).

132. These sources can also be helpful in determining the extent to which TCSPs are able to effectively manage ML/TF risks. Information-sharing and collaboration should take place among AML/CFT supervisors across all sectors (legal professionals, accountants and TCSPs). Supervisors and SRBs should issue guidance to the TCSPs on issues of concern. Guidance should be frequently updated.

133. Competent authorities may also consider undertaking a targeted sectoral risk assessment to get a better understanding of the specific environment in which TCSPs operate in the country and the nature of services provided by them.

134. Supervisors and SRBs should understand the level of inherent risk including the nature and complexity of services provided by the TCSP. Supervisors and SRBs should also consider the type of services the TCSP is providing as well as its size and business model, corporate governance arrangements, the compliance culture within the organisation, financial and accounting information, delivery channels, client profiles, geographic location and countries of operation.

135. Supervisors and SRBs should also consider the controls TCSPs have in place (e.g. the quality of the risk management policy, the functioning of the internal oversight functions and the quality of oversight of any outsourcing and subcontracting arrangements). Supervisors and SRBs should require TCSPs to have group wide programmes against ML/TF, including for sharing of information within the group for AML/CFT purposes. Policies and procedures should be consistently applied and supervised across the group.

136. Supervisors and SRBs should seek to ensure their supervised populations are fully aware of, and compliant with, measures to identify and verify a client, the client's source of wealth and funds where required, along with measures designed to ensure transparency of beneficial ownership, as these are cross-cutting issues which affect several aspects of AML/CFT.

137. Supervisors and SRBs should review their assessment of TCSPs' ML/TF risk profiles periodically, including when circumstances change materially or relevant new threats emerge and appropriately communicate this assessment to the profession.

138. Supervisors and SRBs should ensure that they are properly assessing the risks associated with legal persons and legal arrangements. To further understand the vulnerabilities associated with beneficial ownership, with a particular focus on the involvement of professional intermediaries, supervisors should stay abreast of research papers and typologies published by international bodies.[25] Useful reference include the Joint FATF and Egmont Group Report on Concealment of Beneficial Ownership published in July 2018.

Mitigating and managing ML/TF risk

139. Supervisors and SRBs should take proportionate mitigating measures. Supervisors and SRBs should determine the frequency and intensity of these measures based on their understanding of the ML/TF risks. Supervisors and SRBs should consider the characteristics of the TCSPs, particularly his/her role as a professional intermediary, in particular their diversity and number. It is essential to have a clear understanding of the ML/TF risks: (a) present in the country; and (b) associated with the type of TCSP and their clients, products and services.

140. Supervisors and SRBs assessing the adequacy of the internal controls, policies and procedures should properly take account of the risk profile of TCSPs, and the degree of discretion allowed to them under the RBA.

141. Supervisors and SRBs should develop a means of identifying which TCSPs or group of TCSPs are at the greatest risk of being used by criminals. This involves considering the probability and impact of ML/TF risk. Probability means the likelihood of ML/TF taking place as a consequence of the activity undertaken by TCSPs, or a group of TCSPs, and the environment they operate in. The risk can also increase or decrease depending on other factors:

a) service and product risk (the likelihood that services or products can be used for ML/TF);

b) client risk (the likelihood that customers' funds may have criminal origins);

c) the nature of transactions (e.g. frequency, volume, counterparties);

d) geographical risk (whether the TCSP, its clients or other offices trade in riskier locations); and

e) other indicators of risk are based on a combination of objective factors and experience, such as the supervisor's wider work with the TCSP as well as

25 Such as the FATF, the Organisation for Economic Co-operation and Development (OECD), the World Bank, the IMF and the United Nations Office on Drugs and Crime (UNODC).

information on its compliance history, complaints about the TCSP or about the quality of its internal controls. Other such factors may include information from government/law enforcement sources, whistle-blowers or negative news reports from credible media particularly those related to predicate offences for ML/TF or to financial crimes.

142. In adopting a RBA to supervision, supervisors 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 clients serviced and geographic areas of activities. The setting up of such groupings could allow supervisors to take a comprehensive view of the TCSP sector, as opposed to an approach where the supervisors concentrate on the individual risks posed by the individual firms. If the risk profile of a TCSP within a grouping changes, supervisors may reassess the supervisory approach, which may include removing the TCSP from the grouping.

143. Supervisors or SRBs should also consider the impact, i.e. the potential harm caused if ML/TF is facilitated by TCSPs or group of TCSPs. A small number of TCSPs may cause a high level of harm. This can depend on:

a) size (i.e. turnover), number and type of clients, number of premises, value of transactions etc.), and

b) links or involvement with other businesses (which could affect the susceptibility to being involved in 'layering' activity, e.g. concealing the origin of the transaction with the purpose to legalise the asset).

144. The risk assessment should be updated by supervisors and SRBs on an ongoing basis. The result from the assessment will help determine the resources the supervisor will allocate to the supervision of TCSPs or group of TCSPs.

145. Supervisors or SRBs should consider whether a TCSP meets the ongoing requirements for continued participation in the profession as well as assessments of competence and of fitness and propriety. This will include whether the TCSP meets expectations related to AML/CFT compliance. This will take place both when a supervised entity joins the profession, and on an ongoing basis thereafter.

146. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to differentiate between categories of TCSPs based on various factors such as their client base, countries they deal with and applicable AML/CFT controls etc.

147. Supervisors and SRBs should acknowledge that in a risk-based regime, not all TCSPs will adopt identical AML/CFT controls and that an isolated incident where the TCSP is part of an illegal transaction unwittingly does not necessarily invalidate the integrity of the TCSP's AML/CFT controls. At the same time, TCSPs should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

148. Supervisors and SRBs 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 the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to TCSPs to enable them to enhance their RBA.

Supervision of the RBA

Licensing or registration

149. R.28 requires TCSPs to be subject to regulatory and supervisory measures to ensure their compliance with AML/CFT requirements.

150. R.28 also requires the supervisor or SRB to take the necessary measures to prevent criminals or their associates from being professionally accredited or holding or being the beneficial owner of a significant or controlling interest or holding a management function in relation to a TCSP. This can be achieved through the evaluation of these persons through a "fit and proper" test.

151. A licensing or registration mechanism is one of the means to identify TCSPs who undertake activities specified in R.22 to whom the regulatory and supervisory measures, including the "fit and proper" test should be applied. It also enables the identification of the number of TCSPs for the purposes of assessing and understanding the ML/TF risks for the country, and the action which should be taken to mitigate them in accordance with R.1.

152. Licensing or registration provides a supervisor or SRB with the means to fulfil a "gate-keeper" role over who can undertake those activities specified in R.22. Licensing or registration should ensure that upon qualification, TCSPs are subject to AML/CFT compliance monitoring.

153. The supervisor or SRB should actively identify individuals and businesses who should be supervised by using intelligence from other competent authorities (e.g. FIUs, company registry, tax authority), information from financial institutions and DNFBPs, complaints by the public and open source information from advertisements and business and commercial registries or any other sources which indicate that there are unsupervised individuals or businesses providing the activities specified in R.22.

154. Licensing or registration frameworks should define the activities which are subject to licensing or registration, prohibit unlicensed or unregistered individuals or businesses providing these activities and set out measures for both refusing licences or registrations and for removing "bad actors".

155. The terms "licensing" or "registration" are not interchangeable. Licensing regimes generally tend to operate over financial institutions and impose mandatory minimum requirements based upon Core Principles on issues such as capital, governance, and resourcing to manage and mitigate prudential conduct as well as ML/TF risks on an on-going basis. Some jurisdictions have adopted similar licensing regimes for TCSPs, generally where TCSPs carry out trust and corporate services, to encompass aspects of prudential and conduct requirements in managing the higher level of ML/TF risks that have been identified in that sector.

156. A jurisdiction may have a registration framework over the entire DNFBP sector, including TCSPs or have a specific registration framework for each constituent of DNFBP. Generally, a supervisor or SRB carries out the registration function.

157. The supervisor or SRB should ensure that requirements for licensing or registration and the process for applying are clear, objective, publicly available and consistently applied. Determination of the licence or registration should be objective and timely. A SRB could be responsible for both supervision and for representing the interests of its members. If so, the SRB should ensure that registration decisions are

taken separately and independently from its activities regarding member representation.

Fit and proper tests

158. A fit and proper test provides a possible mechanism for a supervisor or SRB to take the necessary measures to prevent criminals or their associates from owning, controlling or holding a management function in a TCSP.

159. In accordance with R.28, the supervisor or SRB should establish the integrity of every beneficial owner, controller and individual holding a management function in a TCSP. However, the decisions on an individual's fitness and propriety may also be based upon a range of factors concerning the individual's competency, probity, and judgement as well as their integrity.

160. In some jurisdictions, a fit and proper test forms a fundamental part of determining whether to license or register the TCSP and whether on an ongoing basis the licensee or registrant (including its owners and controllers, where applicable) remains fit and proper to continue in that role. The initial assessment of an individual's fitness and propriety is a combination of obtaining information from the individual and corroborating elements of that information against independent credible sources to determine whether the individual is fit and proper to hold that position.

161. The process for determining fitness and propriety generally requires the applicant to complete a questionnaire. It could gather personal identification information, residential and employment history, and require disclosure by the applicant of any convictions or adverse judgements relating to the applicant, including pending prosecutions and convictions. Elements of this information should be corroborated to establish the bona fides of an individual. Such checks could include enquiries about the individual with law enforcement agencies and other supervisors or screening the individual against independent electronic search databases. The personal data collected should be kept confidential.

162. The supervisor or SRB should also ensure on an ongoing basis that those holding or being the beneficial owner of significant or controlling interest in and individuals holding management functions in a TCSP are fit and proper. A fit and proper test should apply to new owners, controllers and individuals holding a management function in a TCSP. The supervisor or SRB should consider re-assessing the fitness and propriety of these individuals arising from any supervisory findings, receipt of information from other competent authorities; or open source information indicating significant adverse developments.

Guarding against "brass-plate" operations

163. The supervisor or SRB should ensure that its licensing or registration requirements require the TCSP to have a meaningful physical presence in the jurisdiction. This usually means that the TCSP should have its place of business in the jurisdiction. Where the TCSP is a legal person, those individuals who form its mind and management should be actively involved in the business and may also be required to be resident in the jurisdiction (although this may not be a necessity provided that there is an appropriate person resident in the jurisdiction who has a responsibility to

report to the supervisor or SRB). A business with only staff who do not possess the professional qualifications and relevant experience to manage the TCSP should not be licensed or registered.

164. A supervisor or SRB should consider the ownership and control structure of the TCSP to determine that sufficient control over its operation will reside within the business, which it is considering licensing, or registering. Factors to take into account could include consideration of where the beneficial owners and controllers reside, the number and type of management functions the TCSP is proposing to have in the country, such as directors and managers, including compliance managers, and the calibre of the individuals who will be occupying those roles. It should also consider the extent to which the TCSP's activities are outsourced to another jurisdiction.

165. The supervisor or SRB should also consider whether the ownership and control structure of TCSPs unduly hinders its identification of the beneficial owners and controllers or presents obstacles to applying effective supervision.

Monitoring and supervision

166. Supervisors and SRBs should take measures to effectively monitor TCSPs through on-site and off-site supervision. The nature of this monitoring will depend on the risk profiles prepared by the supervisor or SRB and the connected RBA. Supervisors and SRBs may choose to adjust:

a) the level of checks required to perform their licensing/registration function: where the ML/TF risk associated with the sector is low, the opportunities for ML/TF associated with a particular business activity may be limited, and approvals may be made on a review of basic documentation. Where the ML/TF risk associated with the sector is high, supervisors and SRBs may ask for additional information.

b) the type of on-site or off-site AML/CFT supervision: supervisors and SRBs may determine the correct mix of on-site and off-site supervision of TCSPs. Off-site supervision may involve analysis of annual independent audits and other mandatory reports, identifying risky intermediaries (i.e. on the basis of the size of the firms, involvement in cross-border activities, or specific business sectors), automated scrutiny of registers to detect missing beneficial ownership information and identification of persons responsible for the filing. It may also include undertaking thematic reviews of the sector, making compulsory the periodic information returns from firms. Off-site supervision alone may not be appropriate in higher risk situations. On-site inspections may involve reviewing AML/CFT internal policies, controls and procedures, interviewing members of senior management, compliance officer and other relevant staff, considering gatekeeper's own risk assessments, spot checking CDD documents and supporting evidence, looking at reporting of ML/TF suspicions in relation to clients, and others matters, which may be observed in the course of an onsite visit and where appropriate, sample testing of reporting obligations.

c) the frequency and nature of ongoing AML/CFT supervision: supervisors and SRBs should proactively adjust the frequency of AML/CFT supervision in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from TCSPs' inclusion in thematic review samples).

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

167. Supervisors and SRBs 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 the existing AML/CFT rules and guidance remain adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to TCSPs to enable them to enhance their RBA.

168. Record keeping and quality assurance are important so that supervisors can document and test the reasons for significant decisions relating to AML/CFT supervision. Supervisors should have an appropriate information retention policy and be able to easily retrieve information while complying with the relevant data protection legislation. Record keeping is crucial and fundamental to the supervisors' work. Undertaking adequate quality assurance is also fundamental to the supervisory process to ensure decision-making/sanctioning is consistent across the supervised population.

Enforcement

169. R.28 requires supervisors or SRB to have adequate powers to perform their functions, including powers to monitor compliance by TCSPs. R.35 requires countries to have the power to impose sanctions, whether criminal, civil or administrative, on DNFBPs, to include TCSPs when providing the services outlined in R.22(e). Sanctions should be available for the directors and senior management of the firms when a TCSP fails to comply with requirements.

170. Competent authorities should use proportionate actions, including a range of supervisory interventions and corrective actions to ensure that any identified deficiencies are addressed in a timely manner. Sanctions may range from informal or written warning, reprimand and censure to punitive sanctions (including suspension or cancellation of registration or licence and criminal prosecutions where appropriate) for more egregious non-compliance, as identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in more severe supervisory response.

171. Enforcement by supervisors and SRBs should be proportionate while having a deterrent effect. Supervisors and SRBs should have (or should delegate to those who have) sufficient resources to investigate and monitor non-compliance. Enforcement should aim to remove the benefits of non-compliance.

Guidance

172. Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement 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 TCSPs should also discuss ML/TF risk within their sector and outline ML/TF indicators and methods of risk assessment to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways which are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction.

173. Where supervisors' guidance remains high-level and principles-based, this may be supplemented by further guidance written by the TCSP sector, which may cover operational issues, and be more detailed and explanatory in nature. Training events may also provide an effective means to ensure TCSPs are aware of and compliance with AML/CFT responsibilities. Where supervisors cooperate to produce combined guidance across sectors, supervisors should ensure this guidance adequately addresses the diversity of roles that come within the guidance's remit, and that such guidance provides practical direction to all its intended recipients. The private sector guidance should be consistent with national legislation and with any guidelines issued by competent authorities with regard to TCSPs and be consistent with all other legal requirements and obligations.

174. Supervisors should consider communicating with other relevant domestic supervisory authorities to secure a coherent interpretation of the legal obligations and to minimise disparities across sectors (such as legal professionals, accountants and TCSPs). Multiple guidance should not create opportunities for regulatory arbitrage. Relevant supervisory authorities should consider preparing joint guidance in consultation with the relevant sectors, while recognising that in many jurisdictions TCSPs will consider that separate guidance targeted at TCSPs will be the most appropriate form.

175. Information and guidance should be provided by supervisors in an up-to-date and accessible format. It could include sectoral guidance material, findings of thematic reviews, training events, newsletters, internet-based material, oral updates on supervisory visits, meetings and annual reports.

176. An SRB should ensure that advice given by the representative side of the organisation correlates to the rules and guidance set by the supervisory side.

Training

177. Training is important for their supervision staff to understand the TCSP sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a TCSP´s ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of AML/CFT policies, procedures and internal controls. It is recommended that the training has a practical basis/dimension.

178. Training should allow supervisory staff to form sound judgments about the quality of the risk assessments made by TCSPs and the adequacy and proportionality of a TCPS´s AML/CFT controls. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Endorsements

179. Supervisors should avoid mandating the use AML systems, tools or software of any third party commercial providers of to avoid conflicts of interest in the effective supervision of firms.

Information exchange

180. Information exchange between the public and private sector and within private sector (e.g. between financial institutions and TCSPs) is important to combat ML/TF. Information sharing and intelligence sharing arrangements between supervisors and public authorities (such as Financial Intelligence Units and law enforcement) should be robust, secure and subject to compliance with national legal requirements.

181. The type of information that could be shared between the public and private sectors include:

a) ML/TF risk assessments;

b) typologies (i.e. case studies) of how money launderers or terrorist financers have misused TCSPs or trusts, companies or other legal entities or arrangements managed by TCSPs;

c) feedback on STRs and other relevant reports;

d) targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with TCSP's as a class or individually; and

e) countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by R.6.

182. Domestic co-operation and information exchange between FIU and supervisors of the TCSP sector and among competent authorities including law enforcement, intelligence, FIU, tax authorities, and TSCP's supervisors is also important for effective monitoring/supervision of the sector. Such co-operation and co-ordination may help avoid gaps and overlaps in supervision and ensure sharing of good practices and findings. Such intelligence should also inform a supervisor's risk-based approach to supervisory assurance. Intelligence about active misconduct investigations and completed cases between supervisors and law enforcement agencies should also be encouraged. When sharing information, protocols and safeguards should be implemented in order to protect sensitive data.

183. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the TCSP sector, taking account of the multi-jurisdictional reach of many TCSP providers.

Supervision of beneficial ownership requirements and source of funds/wealth requirements

184. TCSPs fulfil a key gatekeeper role to the wider financial community through the activities they undertake in the formation of legal persons and legal arrangements and where they are involved in the management and administration of legal persons and legal arrangements.

185. As DNFBPs, they are required to apply CDD measures to beneficial owners of legal persons and legal arrangements to whom they are providing advice or formation services. In a number of countries a TCSP may be required as part of the process of registering the legal person and will be responsible for providing basic and/or beneficial ownership information to the registry.

186. In their capacity as company directors, trustees, nominees or foundation officials etc. of these legal persons and legal arrangements, TCSPs often represent these legal persons and legal arrangements in their dealings with other financial institutions and DNFBPs that are providing for example banking or audit services to these types of customer.

187. These financial institutions and other DNFBPs may request the CDD information collected and maintained by TCSPs, who because of their role as director, nominee or trustee, will act as the principal point of contact with the legal person or legal arrangement. These financial institutions and other DNFBPs may never meet the beneficial owner/s of the legal person or legal arrangement.

188. Under R.28, countries should ensure that TCSPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements, which includes identifying the beneficial owner/s and taking reasonable measures to verify them. Additionally R.24 and R.25 regarding transparency of beneficial ownership of legal persons and legal arrangements, require countries to have mechanisms for ensuring that adequate, accurate and up to date information is available on a timely basis on these legal entities. The FATF and Egmont Group also published the Report on Concealment of Beneficial Ownership in July 2018 which identified issues to help address the vulnerabilities associated with the concealment of beneficial ownership.

189. R.24 and R.25 also require countries to have mechanisms to ensure that information provided to registries is accurate and updated on a timely basis and that beneficial ownership information is accurate and current. To determine the adequacy of a system for monitoring and ensuring compliance, countries should have regard to the risk of AML/CFT in given businesses (i.e. if there is a proven higher risk then higher monitoring measures should be taken). TCSPs must, however, be cautious in blindly relying on the information contained in registries. In addition it is important for there to be some form of ongoing monitoring during a relationship to detect unusual and potentially suspicious transactions as a result of a change in beneficial ownership as registries are unlikely to provide such information on a dynamic basis.

190. In accordance with R.28, TCSPs should be subject to risk-based supervision by a supervisor or SRB covering the beneficial ownership and record-keeping requirements of R.10 and R.11. The Supervisor or SRB should have a supervisory framework which can help in ascertaining that accurate and current basic and

beneficial ownership information on legal person and legal arrangements is maintained and will be available on a timely basis to competent authorities.

191. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which TCSPs have established to identify and record the beneficial owner. In addition, they should undertake sample testing of client files on a representative basis to gauge the effectiveness of the application of those measures and the accessibility of accurate beneficial ownership information.

192. As part of the onsite and offsite inspection, supervisors or SRBs should examine the policies, procedures and controls that are in place for on-boarding of new clients to establish what information and documentation is required where the client is a natural person or legal person or trust or other similar legal arrangements. Supervisors or SRBs should verify the adequacy of these procedures and controls to identify beneficial owners in order to understand the ownership and control structure of these legal person or trust or other similar arrangements and to ascertain the business activity.

193. Sample testing of client files will also assist the supervisor or SRB in determining whether controls are effective for the accurate identification of beneficial ownership, accurate disclosure of that information to relevant parties and for establishing if that information is readily available. The extent of testing will be dependent on risk but the files selected should reflect the profile of the client base and include both new and existing clients.

194. Supervisors or SRBs should also consider the measures the TCSP has put in place for monitoring changes in the beneficial ownership of legal person or trust or other similar arrangements to whom they provide services or act to ensure that beneficial ownership information is accurate and current and to determine how timely updated filings are made, where relevant to a registry.

195. During examinations, supervisors or SRBs should consider whether to verify the beneficial ownership information available on the files of the TCSP with that held by the relevant registry, if any.

196. Supervisors or SRBs may also take into account information from other competent authorities such as FIUs public reports and information from other financial institutions or DNFBPs, to verify the efficacy of the TCSP’s controls.

197. TCSPs should be subject to risk-based supervision by a supervisor or SRB covering the requirements to identify and evidence the source of funds and source of wealth for higher risk clients to whom they provide services. The supervisor or SRB should have the supervisory framework, which can help in ascertaining that accurate and current information on sources of funds and wealth is properly evidenced and available on a timely basis to competent authorities. The supervisor or SRB should analyse the adequacy of the procedures and the controls, which TCSPs have established to identify and record sources of wealth in arrangements.

Nominee arrangements

198. A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the beneficial owner. A nominee

shareholder is a natural or legal person who is officially recorded in the Register of Members (shareholders) of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the beneficial owner. The shares may be held on trust or through a custodial agreement. This nominee relationship should be disclosed to the company and to any relevant registry.

199. In a number of countries, TCSPs act or arrange for other persons (either individuals or corporate) to act as directors and act or arrange for other persons (either individuals or corporate) to act as a nominee shareholder for another person as part of their professional services. In accordance with R.24, these TCSPs should be subject to licensing/registration and supervision, and where acting as nominee shareholder, their status disclosed.

200. There will be legitimate reasons for a TCSP to act as or provide directors to a legal person or act or provide nominee shareholders. It should be apparent from the records of the legal person that it is the TCSP fulfilling these roles as the identity of the TCSP, or that of its members of staff will be disclosed on the register of directors, register of members for example.

201. There are legitimate reasons for a company to have a nominee shareholder including for the settlement and safekeeping of shares in listed companies where post traded specialists act as nominee shareholders. Company law may impose requirement for a legal person to have more than one member, which may also give rise to nominee arrangements. However, these nominee director and nominee shareholder arrangements can be misused to hide the identity of the true beneficial owner/s of the legal person. There may be individuals prepared to lend their name as a director or shareholder of a legal person on behalf of another without disclosing the identity of, or from whom, they will take instructions or whom they represent. They are sometimes referred to as "strawmen".

202. Nominee directors and nominees shareholders can create obstacles to identifying the true beneficial owner/s of a legal person, particularly where their status is not disclosed. This is because it will be the identity of the nominee, which is disclosed in the corporate records of the legal person held by a registry and in the company records at its registered office. Company law in a number of countries does not recognise the status of a nominee director because in law it is the directors of the company who are liable for its activities and the directors have a duty to act in the best interest of the company.

203. Supervisors and SRBs should be alert to the possibility that undisclosed nominee arrangements may exist. They should consider as part of their onsite and offsite inspections and examination of the policies, procedures and controls and client records of the TCSP whether undisclosed nominee arrangements would be identified and addressed as part of the CDD process and ongoing monitoring by the TCSP.

204. An undisclosed nominee arrangement may exists where there are the following (non-exhaustive) indicators:

a) the profile of a trustee, director or shareholder is inconsistent with the activities of the trust, company or other legal entity;

b) the individual holds a number of appointments to unconnected trusts, companies or other legal entities;

c) a nominee's source of wealth is inconsistent with the value and nature of the assets within the trust, company or other legal entities;

d) funds into and out of the trust, company or other legal entity are sent to or received from unidentified third party/ies;

e) the TCSP is accustomed to acting on the instructions of another person who is not the trustee or director or other natural person exercising effective control; and

f) Requests or instructions are subject to little or no scrutiny and/or responded to extremely quickly without challenge by the individual/s purporting to act as the trustee, director/s or other natural person exercising effective control.

Annex 1: Beneficial ownership information in relation to a trust or other legal arrangements to whom a TCSP provides services

1. Taking a RBA, the amount of information that should be obtained by the TCSP will depend on whether the TCSP is establishing or administering the trust, company or other legal entity or is acting as or providing a trustee or director of the trust, company or other legal entity. In these cases, a TCSP will be required to understand the general purpose behind the structure and the source of funds in the structure in addition to being able to identify the beneficial owners and controlling persons. A TCSP which is providing other services (e.g. acting as registered office) to the trust, company or other legal entity will, taking a risk based approach, be required to obtain sufficient information to enable it to be able to identify the beneficial owners and controlling persons of the trust, company or other legal entity.

2. A TCSP that is not acting as trustee may, in appropriate circumstances, rely on a synopsis prepared by another TCSP, a legal professional or accountant providing services to the trust or relevant extracts from the trust deed itself to enable the TCSP to identify who is the settlor, trustees, protector (if any), beneficiaries or natural persons exercising effective control. This is in addition to the requirement, where appropriate, to obtain evidence to verify the identity of such persons as discussed below.

In relation to a trust

3. A TCSP should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that the TCSP's policies should enable it to disregard source documents, data or information which are perceived to be unreliable)

   i. the settlor;
   ii. the protector;
   iii. the trustee(s), where the TCSP is not acting as trustee;
   iv. the beneficiaries or class of beneficiaries, and
   v. any other natural person actually exercising effective control over the trust.

Settlor

a) A settlor is generally any person (or persons) by whom the trust was made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the settlor must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration).

b) A settlor may or may not be named in the trust deed. TCSPs should have policies and procedures in place to identify and verify the identity of the real economic settlor.

c) A TCSP establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a trustee, company or other legal entity should have policies and procedures in place (taking a risk based approach) to identify the source of funds in the trust, company or other legal entity.

d) It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift, letter of wishes etc.

e) Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

Beneficiaries

a) A TCSP should have policies and procedures in place, adopting a RBA to enable it to form a reasonable belief that it knows the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that the TCSP is satisfied that it knows who the beneficiaries are. This does not require the TCSP to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the TCSP should at least identify and verify the identity of beneficiaries who have current fixed rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).

b) Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), a TCSP should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

c) Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries are minors under the law governing the trust, although a TCSP should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed) the TCSP is not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary.

d) In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, TCSPs are not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary.

e) TCSPs who administer the trust or company or other legal entity owned by a trust or otherwise provide or act as trustee or director to the trustee, company or other legal entity should have procedures in place so that there is a requirement to update the information provided if named beneficiaries are added or removed from the class of beneficiaries, or beneficiaries receive distributions or benefits for the first time after the information has been provided, or there are other changes to the class of beneficiaries.

f) TCSPs are not obliged to obtain other information about beneficiaries other than to enable the TCSP to satisfy itself that it knows who the beneficiaries are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust is a PEP.

Natural person exercising effective control

a) A TCSP providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust.

b) For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

   i. dispose of or invest (other than as an investment manager or adviser) trust property;

   ii. direct, make or approve trust distributions;

   iii. vary or terminate the trust;

   iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and or;

   v. appoint or remove trustees.

c) TCSPs who administer the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above.

Corporate settlors and beneficiaries

4. These examples are subject to the more general guidance on what information should be obtained by the TCSP to enable it to identify settlors and beneficiaries. It is not intended to suggest that a TCSP must obtain more information about a beneficiary which is an entity where it would not need to obtain such information if the beneficiary is an individual.

a) In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, the TCSP should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.

b) In the case of a settlor which is a legal entity, the TCSP should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, the TCSP should take steps to satisfy itself as to the identity of the economic settlor of the trust (i.e. the person who has provided funds to the legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor retains powers over the trust (e.g. a power of revocation), the TCSP should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

c) In the case of a beneficiary which is an entity (e.g. a charitable trust or company), the TCSP should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the TCSP should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate trustee

a) Where a TCSP is not itself acting as trustee, it is necessary for the TCSP to obtain information to enable it to identify and verify the identity of the trustee(s) and, where the trustee is a corporate trustee, identify the corporate, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.

b) Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body which regulates the trustee and of the regulated trustee itself).

c) It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are typically called private trust companies and may have a restricted trust licence which enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the TCSP should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the TCSP does not need to obtain detailed information to identify the directors or controlling persons of that entity which acts as shareholder of the private trust company.

Individual and Corporate protector

a) Where a TCSP is not itself acting as a protector and a protector has been appointed, it is necessary for the TCSP to obtain information to enable it to identify and verify the identity of the protector

b) Where the protector is a legal entity, the TCSP should obtain sufficient information that it can satisfy itself who is the controlling person and beneficial owner of the protector, and take reasonable measure to verify their identity.

c) Where the protector is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain to satisfy itself as to the beneficial owner of the regulated protector (e.g. the web-site of the body that regulates the protector and of the regulated protector itself).

Annex 2: Glossary of terminology

Beneficial Owner

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

Competent Authorities

Competent authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

a) Casinos (which also includes internet and ship based casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

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

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

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

- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).'

FATF Recommendations

Refers to the FATF Forty Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with a legal professional or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term *"Legal professional"* refers to lawyers, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Red Flags

Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A "red flag" may be used as a short hand for any indicator of risk which puts an investigating TCSP on notice that further checks or other appropriate safeguarding actions will be required.

Self-regulatory bodies (SRB)

A *SRB* is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Supervisors

Supervisors refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("financial supervisors" 90) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Annex 3: Supervisory practices for implementation of the RBA to TCSPs[26]

The Group of International Finance Sector Supervisors (GIFCS)

Originally known as the Offshore Group of Banking Supervisors, GIFCS was formed in 1980 at the instigation of the Basel Committee on Banking Supervision. Whilst maintaining a close working relationship with the Basel Committee, the group now represents the interests of its member jurisdictions in the supervision of banks, collective investment funds, securities activities and TCSP sectors. GIFCS, which represents supervisory authorities of 20 regional and international finance centres, issued a Standard for the Regulation of TCSPs which sets a minimum benchmark for the effective supervision of the sector, incorporating licensing requirements, together with principles for AML/CFT, prudential and governance supervision of the sector. https://www.groupgifcs.org/letsgo/uploads/gifcsstandardontcsps.pdf

The Standard contains principles for supervision, and specifically includes requirements that the supervisor:

- Assesses at the time of licensing and on an ongoing basis whether a TCSP, its controllers, directors, partners, and Money Laundering Reporting and Compliance Officers are fit and proper,
- Considers the ownership, structure, control and management of the TCSP ensuring that that the ownership structure does not hinder effective supervision or facilitate regulatory arbitrage,
- Requires a TCSP to demonstrate physical presence in the jurisdiction in which it is being regulated which would be demonstrated by requiring its "mind and management" being resident in the jurisdiction and actively involved in the TCSP's governance and having an operational place of business in the jurisdiction,
- Requires that a TCSP embeds a robust corporate governance culture and risk management framework,
- Ensures that a TCSP has ongoing effective management and/or administrative control mechanisms over legal persons and legal arrangements for which its acts, particularly in relation to ultimate beneficial ownership and ensuring that full documentation and information is held on the activity of those vehicles, and
- Ensures that a TCSP has controls to prevent it becoming engaged directly or indirectly with bribery and corruption.

26 The Hong Kong Institute of Chartered Secretaries (HKICS) has issued an updated guidance to TCSP sector. This is available at: www.hkics.org.hk/media/publication/attachment/PUBLICATION_A_2380_HKICS_AML_CFT_Guideline.pdf. Further, the British Virgin Islands'(BVI's) Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code of Practice, 2018 is available at: www.bvifsc.vg/sites/default/files/anti-money_laundering_and_terrorist_financing_amendment_no._2_code_of_practice_2018.pdf

The Standard also underpins the FATF Recommendations and has a particular focus for supervisors on national and international cooperation and information sharing and ensuring the effective implementation by a TCSP of targeted financial sanctions. All its members are committed to meeting the Standard. A process to evaluate its members' compliance with Standard commenced in 2016.

Guernsey

Guernsey is an international finance centre with a significant TCSP sector which has been subject to prudential and AML/CFT supervision since 2001. The Guernsey Financial Services Commission ("the Commission") is the competent authority in the Bailiwick of Guernsey for licensing and supervising Trust and Corporate Service Providers ("TCSPs).

Under the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000 all licensed TCSPs must at the outset and on an ongoing basis meet a minimum criteria for licensing. This criteria includes a transparent ownership structure, capital adequacy, suitable experience and favourable track record, a suitable risk management framework, sufficient staffing and systems resources, and at least two directors resident in Guernsey who are independent of each over and of appropriate standing and experience to effectively direct and apply "four eyes" control over the business.

Within this criteria, the TCSP and each individual occupying the role of controller (including beneficial owners), partner, director or manager must at the outset and on an ongoing basis meet a fit and proper test covering competence, probity (encompassing their integrity, honesty and reputation), experience, professionalism, soundness of judgement and solvency. Individuals must complete an extensive personal questionnaire recording their employment record, professional qualifications, personal business interests and records regarding any bankruptcy proceedings and any criminal, regulatory or disciplinary sanctions or pending cases.

All licence applications are subject to careful scrutiny. The Commission has statutory powers to impose sanctions against a TCSP or an individual where it considers that the minimum licensing criteria, including the fit and proper criterion, is not or has not been met. Those powers include the power to revoke licences, prohibit individuals from holding a position in the finance sector, impose fines and issue public statements where this criteria is not met. The Commission has published its policy to enforce and use such powers where the failings are sufficiently serious that addressing deficiencies through ordinary or enhanced supervisory processes are not appropriate.

Examples of supervisory action

Example 1 (Refusal of licence application)

An application for a licence was made to establish a TCSP services. Its business model contained a number of significant inherent higher risk factors including proposals to offer "family office" services and yacht administration to high net worth individuals based in jurisdictions identified by credible sources as at a higher risk of bribery and corruption. It also included jurisdictions which had yet to implement international tax standards on exchange of information.

The application raised the following concerns:

- The applicant proposed having two executive directors. One of the directors would work full time and the other who would give 20% of his normal working week to the business of the applicant but stating that he would increase his hours if necessary. However this director had a large number of other unrelated business interests which could limit the amount of time that he could devote to the applicant's business. The Commission was therefore concerned that there would be lack of effective challenge to the one full time director and limited "four-eyes" control over the applicant's business, a key tenant of the minimum licensing criteria.

- The quality of the application made by the applicant was extremely poor, exhibiting a lack of awareness of the requirements regarding minimum capital and insurance cover for TCSPs together with key information missing on financial forecasts and operating policies and procedures, demonstrating lack of professionalism and skill to provide trust and corporate services. The Commission was not satisfied that the applicant and its directors met the fit and proper test.

The Commission issued a notice that it was "minded to refuse the application" on the grounds that the applicant did not meet the minimum licensing criteria. The application was subsequently withdrawn.

Example 2 (enforcement)

The Commission imposed sanctions against four individuals who were controllers (owners) and directors of a TCSP, and against a fifth individual who was its independent non-executive director, after identifying during an onsite inspection significant failings in the TCSP's anti-money laundering and countering terrorist financing systems and controls. The individuals had failed to ensure that TCSP met the following regulatory requirements of Guernsey AML/CFT regime:-

- To undertake and regularly review relationships risk assessments

- To always take reasonable measures to identify and verify customers and beneficial owners or to obtain information on the purposes and intended nature of each business relationship

- To always undertake enhanced customer due diligence on customers assessed as high risk

- To perform ongoing and effective monitoring of its existing business relationships

- To have appropriate and effective procedures to ensure compliance with legislation for disclosing suspicious activity

The Commission had previously identified similar failings within the TCSP which it had been required to remediate and which had not been appropriately actioned in all instances. As a consequence of these failings the Commission concluded that the individuals had failed to understand the legal and professional obligations upon them as controllers and directors of a TCSP. In failing to remedy previously identified deficiencies the individuals had acted without sound judgement required as part of the fit and proper criterion.

The four executive directors were each fined £50,000 and the non-executive director was fined £10,000. Three of the executive directors were prohibited from acting as a controller, partner, director or money laundering reporting officer within the Bailiwick's finance industry for five years. A public statement was issued identifying the individuals, providing information on the case and the sanctions which were applied.

Example 3 (enforcement)

A TCSP and three of its directors were sanctioned by the Commission for failing to implement appropriate and effective polices, procedure and controls to mitigate ML/TF risks to which the business could be exposed. An onsite inspection identified fundamental failings in the TCSP's anti-money laundering and countering of terrorist financing systems and controls, particularly in respect of business relationships assessed as high risk involving politically exposed persons ("PEPs") linked to higher risk jurisdictions. The failings were referred to the Commission's Enforcement Division to undertake further investigation which carried out a further onsite inspection.

The Commission identified the following failings:

- That the TCSP failed to conduct customer due diligence in accordance with regulatory requirements, and in respect of individuals to whom a Power of Attorney had been granted or were potential beneficiaries of trusts;
- That the TCSP failed to undertake sufficient enhanced customer due diligence, including taking reasonable measures to establish source of wealth and funds of customers who were PEPs and had links to jurisdictions identified by credible sources as having a higher risk of bribery and corruption;
- That the TCSP failed to effectively monitor ongoing customer activity or scrutinise unusual transactions.

The failings were similar to deficiencies identified in two previous inspections to the TCSP and showed that the remedial action that it had been required to undertake had not been appropriately actioned in all instances. The Commission concluded that the TCSP's systems and controls did not enable it to comply with Guernsey's AML/CFT regulatory requirements and therefore the TCSP had not conducted its business in a prudent manner required by the minimum licensing criteria. The Commission considered that the Directors had demonstrated a lack of probity, competence and soundness of judgement which are factors which are taken into account when considering whether a director is a fit and proper person.

The firm was fined £42,000, one of the directors who served as the compliance director and money laundering reporting officer was fined £18,375 and the two other directors were each fined £10,500. A public statement was issued identifying the parties, providing information on the case and the sanctions which were applied.

Hong Kong, China

Priority is given to and more resources are accorded to higher risk cases for targeted inspection. For higher risk cases, on-site inspections are conducted on a priority basis and the TCSP licensees are subject to more frequent compliance inspections to ensure their continuous compliance with the statutory CDD and record-keeping requirements. Customer and transaction records are checked during the on-site inspections to ensure that effective AML/CFT measures are in place for compliance with the statutory requirements. For higher risk cases, a higher proportion of such records will be selected for checking.

Also, applicants for TCSP licences and licensees are required to complete a supplementary information sheet to provide the relevant information in order to monitor their compliance with the AML/CFT requirements and to assess their ML/TF risks. Off-site supervision consists of analysis of the supplementary information sheets and ongoing monitoring of the compliance of the licensing conditions of the licensees, including compliance with AML/CFT requirements, classifying the risk profiles of individual licensees, identifying risky applicants/licensees, undertaking thematic reviews of the sector and meeting with trade representatives to monitor and assess any changes in the trade practice. Follow-up actions, including prosecution and disciplinary action, will be taken if any non-compliance with statutory CDD and record keeping requirements is identified.

Examples of supervisory action

Example 1

An application for TCSP licence was made by Corporation A. Ms B was the sole director and ultimate owner of Corporation A. She was also named as Corporation A's Compliance Officer and the Money Laundering Reporting Officer. The Companies Registry (CR) conducted on-site inspection on Corporation A to interview Ms B and inspect transaction records of Corporation A. During the inspection, Ms B was unable to produce any record or document and there was no evidence showing that Ms B as the Compliance Officer and the Money Laundering Reporting Officer was normally based in Hong Kong.

Upon consideration of all the circumstances of the case including the non-compliances above, the CR was not satisfied that Ms B was fit and proper to carry on or be associated with a TCSP business. As a result, Corporation A's application for TCSP licence was rejected.

Example 2

A group of five TCSPs operating at the same business premises applied for TCSP licences. They provided company services to a very large number of customers and acted as the company secretaries of over 70 000 companies. A Mr X was the ultimate owner and director of the five TCSPs, and was also the Compliance Officer and Money Laundering Reporting Officer of these TCSPs.

Some of these TCSPs were checked to be the company secretaries of front companies suspected of having business or connection with entities subject to the United Nations Security Council sanctions.

The CR conducted on-site inspection at the business premises and inspected records of the TCSPs' customers and transactions. Mr X was interviewed. All five applicants and Mr X failed to demonstrate that they were fit and proper to carry on or be associated with a TCSP business. They also failed to demonstrate that they had complied with the statutory CDD and record-keeping requirements. Eventually, all the five applicants had withdrawn their applications for TCSP licences before CR proceeded to reject their applications.

Isle of Man

Through the Beneficial Ownership Act 2017 (the "Act"), the Isle of Man established a Beneficial Ownership Register held by the Companies Registry and overseen by the Isle of Man Financial Services Authority. This legislation compliments longstanding requirements upon FIs and DNFBPs to undertake customer due diligence requirements including beneficial owners of their customers.

From 1st July 2017 the Act placed legal obligations on certain types of legal persons, their beneficial owners, intermediate owners, legal owners and nominated officers with regard to beneficial ownership information, namely that beneficial ownership information should be passed through the ownership chain to the legal person's nominated officer. The legal person's nominated officer must retain all beneficial owners' details, and add any beneficial owners holding more than 25% ownership or control to the beneficial ownership database. The Act does not apply to legal persons which are foreign companies, a company listed on a recognised stock exchange or entities wholly owned by a company listed on a recognised stock exchange.

The FSA has powers in order to ascertain whether the obligations and requirements imposed by the Act have been and are being complied with and whether the database is effective and its information accurate. The following case example provides an example of supervisory action:

Members of the FSA's Enforcement Division conducted an inspection in relation to 10 companies which had a common nominated officer. The nominated officer was visited and the information held by them checked against the submissions made to the beneficial ownership database. Minor errors were identified in relation to two companies whereby the nature of ownership was recorded incorrectly and the trustees of a trust had not been considered as beneficial owners of the underlying Isle of Man company. The Authority issued a report identifying the errors, detailing how the nominated officer should regularise them and a deadline for which the corrections must be made. The database was updated by the nominated officer in the given timescale.

Jersey

Supervising TCSP's business/enterprise risk assessment

The Jersey Financial Services Commission (JFSC) received a response from a regulated TCSP to queries the JFSC raised over its risk assessment. The response provided details of a 'cash register' and cash transactions undertaken on behalf of its customers. Owing to the inherent ML risk relating to these transactions, the TCSP was formally placed under investigation, encompassing a 6-day onsite examination with Enforcement and Supervision reviewing corporate governance, the compliance function and conduct of business, with particular focus to those customers identified on the cash register. Following the on-site examination the JFSC made the following observations:

The regulated TCSP appeared to have committed significant breaches of the TCSP Code of Practice;

Contrary to legal and regulatory requirements, the TCSP had carried out cash transactions where it did not hold adequate CDD, Source of Funds or rationale for services being carried out.

The TCB was informed that the JFSC was concerned that it may have facilitated money laundering on an extensive scale, for which suspicious activity reports were submitted. Directions were issued to each principal person restricting their involvement in Jersey's finance industry, along with the issuance of a public statement in respect of the TCSP and the Principals

Examples of supervisory actions

Example 1

The JFSC undertook an onsite examination to a TCSP and identified deficiencies related to corporate governance, effectiveness of compliance function and AML/CFT issues, which included ineffective procedures, transaction monitoring deficiencies, lack of CDD/Source of Funds (including on PEPs), lack of AML/CFT awareness/training and deficient record keeping. As a result of these deficiencies, the JFSC issued a Notice requiring the appointment of a reporting professional to review a larger sample of client files. The reporting professional's findings replicated to a large extent the JFSC's findings.

Whilst the Reporting Professional's review was being undertaken, the JFSC became aware of a Notice on a foreign regulator's website regarding an action that was being taken in relation to a company that had a connection to a company that the Reporting Professional was reviewing. Contact was made with the foreign regulator and a meeting was held. Assistance was also provided to law enforcement authority from the foreign jurisdiction concerned regarding a fraud perpetrated there but where the proceeds of the fraud were received by the TCSP. Perpetrators of the fraud were jailed in the UK. The business was sold to another TCSP and the JFSC issued a public statement and placed restrictions on the Principal Persons by directions.

Example 2

The JFSC conducted a supervisory on-site examination of a regulated TCSP, which identified a number of significant concerns over corporate governance and its provision of services to structures under administration. An internal remediation process was undertaken and a regulatory consulting firm was engaged to perform an independent review of the corporate governance and customer files in respect of the trust company business. The regulated TCSP also promptly implemented initial steps in relation to training and revised policies and procedures to remediate issues identified.

Following the on-site examination, the JFSC required co-signatories to be appointed to review and pre-approve certain transactions. The co-signatories were required to provide a report of any issues identified during the course of their engagement. Two individuals responsible for approx. 70% of the trust and corporate business clients voluntarily took a leave of absence and subsequently left.

The on-site examination, co-signatories report and consultants report identified a lack of effective governance and lack of appropriate compliance oversight in relation to the trust company business. This resulted in the two individuals receiving banning directions and a public statement being issued in respect of the regulated TCSP and both individuals. Following the conclusion of the investigation, the regulated TCSP underwent intense remediation, monitored by the JFSC.

Example 3

During an on-site examination serious concerns were noted in relation to the conduct of the TCSP and its principal persons in the provision of services to a customer structure. The matter was referred to the Enforcement Division and an investigation was commenced, which identified a number of failings on behalf of the TCSP and its principal and key persons in relation to the customer structure. In order to assess whether the failings were inherent across the wider business, the JFSC required the TCSP to appoint an independent reporting professional to conduct a wider review of customer structures. The investigation and the reporting professional's report both identified a lack of effective governance surrounding, and inadequate systems and controls in respect of the TCSP's obligations under the AML/CFT regime on issues related to obtaining sufficient CDD; applying correct customer risk ratings; understanding and documenting customer rationale, fully understanding source of wealth/source of funds; exercising control and understanding the complexity of risks; implementing a robust annual review process; considering and acting upon adverse information; poor record keeping and failing to consider obligations under the AML/CFT legislation to with regards to suspicious activity reporting

The JFSC issued directions requiring remediation and to the principal and key persons requiring further AML/CFT training.

Example 4

The JFSC was notified of a number of regulatory breaches namely four breaches of Section 8.3.1 of the AML/CFT Handbook, the late notification and internal reporting to the MLRO of suspicion relating to customers. As a result of the late notification of the breaches, the TCB was issued with Civil Penalty warning. Given the nature of the breaches, the matter was referred to Enforcement for consideration, who made the Jersey FIS aware of concerns over failing to report and late submission of SARs.

In agreement with the JFSC, the TCSP appointed a reporting professional voluntarily to conduct a review of its remediation of issues and compliance function.

The report produced alleviated much of the JFSC's concerns concerning the current compliance environment however there was still some remediation required. The matter was passed back to Supervision for monitoring of the remediation and to test at a later stage. The TCSP was notified that the JFSC would consider a Band 2 Civil Penalty should the issues not be remediated satisfactorily.

Example 5

As a result of an on-site examination, concerns were highlighted over the competency of the MLRO in AML/CFT at a TCSP. Specifically it appeared that the MLRO had failed to externalise a number of internal SARs in circumstances where he noted suspicion of criminality.

Following a referral from Supervision, Enforcement conducted an investigation in respect of the MLRO's fitness and propriety. The investigation concluded that the MLRO lacked competency in AML/CFT matters but did not lack integrity.

A without prejudice settlement was entered into with the MLRO, restricting him from acting in any Key Person role until such time he completed further AML/CFT training. As a result of the Enforcement action, the TCB appointed a new MLRO.

Malaysia

A. Fit and Proper Requirements

Trust service providers in Malaysia consist of trust companies registered under the Trust Companies Act 1949 or incorporated under the Public Trust Corporation Act 1995. Company service providers are made up of members of professional bodies or individuals licensed by the Companies Commission of Malaysia. All TCSPs are subject to appropriate market entry controls under the respective legislation and professional obligations governing them, by which they are required to fulfil certain fit and proper requirements.

B. AML/CFT Risk-based Supervision – Bank Negara Malaysia (BNM)

Under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), BNM is the designated competent authority for the AML/CFT supervision of the DNFBPs, including TCSPs. BNM adopts a risk-based approach supervision on TCSPs, in which the differentiation is guided by the outcome of the National Risk Assessment (NRA) and the application of Risk-Based Supervisory Framework (D'SuRF), as follows:

i. National Risk Assessment (NRA) 2017

Malaysia's third iteration of the NRA in 2017 comprising assessment of ML/TF inherent risk and overall control effectiveness stipulated the TCSPs' net ML and TF risks as **"MEDIUM HIGH"** and **"MEDIUM"** level, respectively, as exacerbated by the sector's marginal control, as follows:

ML		TF	
Inherent Risk	Medium	Inherent Risk	Low
Control	Marginal	Control	Marginal
Net Risk	Medium High	Net Risk	Medium

i. Risk-Based Supervisory Framework for DNFBPs and Other Financial Institutions (D'SuRF)

D'SuRF encapsulates end-to-end governance and supervisory process, risk-based application of supervisory tools. In line with the ML/TF rating of the sector and the application of D'SuRF, the frequency and intensity of monitoring on TCSPs are guided accordingly to include a range of supervisory tools, which include the following:

- **On-site Examination**

Firms are selected based on a robust selection process under the D'SuRF, which is in line with the risk profile of the reporting institutions (RIs). The on-site examination is in-depth, with assessments covering the RIs' inherent risk and quality of risk management. In applying RBA, BNM imposes post-onsite follow-up measures for RIs with heightened risks. This includes requiring the RI to submit proposals to BNM on planned measures to rectify any supervisory issues and progress report until full rectification. The D'SuRF sets the deadline for both submissions. The follow-up measures have been imposed on a number of TCSPs selected for on-site examination.

- **Off-site Monitoring and Supervisory Outreach Activities**

In addition, BNM employs a range of off-site monitoring and supervisory outreach activities, aimed to elevate awareness and guide the implementation of the AMLA requirements by the TCSPs. These off-site tools are also deployed according to the RBA, whereby the intensity and frequency for the TCSPs is relatively higher compared to other sectors. Among the off-site monitoring, includes the submission of data and compliance Report, internal audit reports, and statistical data. BNM and the relevant SRBs also conduct periodic nationwide AML/CFT outreach and awareness programmes.

Monaco

Monaco completed its first NRA (National Risk Assessment) in 2017 and the CSPs were included in the scope (see public NRA report in www.siccfin.mc/en/The-National-Risk-Assessment-NRA).

The assessed risk regarding CSPs was rated MH (moderate high) so the CSP are included in the priority professionals to be inspected on-site. There are about 40 CSPs in Monaco so ten to twelve inspections are planned every year. In addition, the CSPs are subject to a compulsory annual questionnaire which they have to send to SICCFIN by February 28, which helps the supervisor in detecting anomalies in their activities. The RBA is not yet fully formalized, but the selection of CSPs to be added to the inspection planning is performed as follows:

- The date of the previous inspection
- The conclusions of the previous inspection and how the CSP responded to it (improvements implemented)
- The evolution of the CSP as detected through the annual questionnaire
- Information transmitted by the FIU (which is within SICCFIN as well as the supervision of professional submitted to AML act) regarding the quality of SARs and other related topics.

Other criteria are planned to be added in the near future.

Singapore

Singapore's Registered Filing Agents and Registered Qualified Individuals Regulatory Regime

Since 2015, firms and companies which intend to incorporate legal entities on behalf of another person or provide corporate services (e.g. acting or arranging for someone to act as director, secretary, shareholders or providing registered office addresses) in the course of their business, must register with the Accounting and Corporate Authority (ACRA) as a Registered Filing Agent (RFA). These firms have to act through at least one Registered Qualified Individual (RQI) with ACRA. Lawyers and accountants are supervised by their respective regulators/regulatory bodies, but if the accountancy or law firm also provides corporate services, it also needs to be registered with ACRA as a RFA and will be subjected to ACRA's AML/CFT requirements in their role as a RFA.

These firms will not be permitted to register as a RFA if any of the firm's beneficial owners, directors, partners or managers have been convicted of criminal offences or if they are undischarged bankrupts. An individual will not be permitted to be registered as a RQI if he/she has been convicted of a criminal offence (especially those related to fraud or dishonesty) or if he is an undischarged bankrupt.

Since 15 Nov 2018, ACRA has enhanced the RFA's registration requirements to mandate anyone seeking registration or renewal as a RFA, to complete a prescribed AML/CFT training programme and also pass a proficiency test once every two years as a pre-condition to their registration or renewal. This seeks to ensure that RFAs can adequately comply with AML/CFT obligations through continuous education.

Annex 4: Members of the RBA Drafting Group

FATF members and observers	Office	Country/Institution
Sarah Wheeler (Co-chair)	Office for Professional Body AML Supervision (OPBAS), FCA	UK
Sandra Garcia (Co-chair)	Department of Treasury	USA
Erik Kiefel	FinCen	
Helena Landstedt and Josefin Lind	County Administrative Board for Stockholm	Sweden
Charlene Davidson	Department of Finance	Canada
Viviana Garza Salazar	Central Bank of Mexico	Mexico
Fiona Crocker	Guernsey Financial Services Commission	Group of International Finance Centre Supervisors(GIFCS)
Ms Janice Tan	Accounting and Regulatory Authority	Singapore
Adi Comeriner Peled	Ministry of Justice	Israel
Richard Walker	Financial Crime and Regulatory Policy, Policy & Resources Committee	Guernsey
Selda van Goor	Central Bank of Netherlands	Netherlands
Natalie Limbasan	Legal Department	OECD
	Accountants	
Member	Office	Institution
Michelle Giddings (Co-chair)	Professional Standards	Institute of Chartered Accountants of England & Wales
Amir Ghandar	Public Policy & Regulation	International Federation of Accountants
	Legal professionals and Notaries	
Member	Office	Institution
Stephen Revell (Co-chair)	Freshfields Bruckhaus Deringer	International Bar Association
Keily Blair	Economic Crime, Regulatory Disputes department	PWC, UK
Mahmood Lone	Regulatory issues and complex cross-border disputes	Allen & Overy LLP, UK
Amy Bell	Law Society's Task Force on ML	Law Society, UK
William Clark	ABA's Task Force on Gatekeeper Regulation and the Profession	American Bar Association (ABA)
Didier de Montmollin	Founder	DGE Avocats, Switzerland
Ignacio Gomá Lanzón	CNUE's Anti-Money Laundering working group	Council of the Notariats of the European Union (CNUE)
Alexander Winkler	Notary office	Austria
Rupert Manhart	Anti-money laundering Committee	Council of Bars and Law Societies of Europe
Silvina Capello	UINL External consultant for AML/CFT issues	International Union of Notariats (UINL)

	TCSPs	
Member	**Office**	**Institution**
John Riches (Co-chair) Samantha Morgan	RMW Law LLP	Society of Trust and Estate Practitioners (STEP)
Emily Deane	Technical Counsel	
Paul Hodgson	Butterfield Trust (Guernsey) Ltd	The Guernsey Association of Trustees
Michael Betley	Trust Corporation International	
Paula Reid	A&L Goodbody	A&L Goodbody, Ireland

GUIDANCE FOR A RISK-BASED APPROACH

TRUST AND COMPANY SERVICE PROVIDERS

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.

This guidance highlights the need for a sound assessment of the money laundering and terrorist financing risks that trust and company service providers face so that the policies, procedures and initial and ongoing client due diligence measures can mitigate these risks.

The FATF developed this non-binding guidance with significant input from the TCSP sector, to ensure that it reflects their practical expertise and good practices.

www.fatf-gafi.org | June 2019