DRAFT REVISED GUIDANCE

FOR A RISK-BASED APPROACH FOR THE BANKING SECTOR

INTRODUCTION

A. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[1]. The FATF has reviewed its RBA guidance for banks and is currently reviewing other RBA guidance papers, all based on the 2003 Recommendations,[2] in order to bring them in line with the new requirements[3] and to incorporate lessons learnt by public authorities and the private sector.

2. [Some words about the process and organisations participating for the banking sector.]

3. The FATF adopted this updated RBA Guidance for the banking sector *[at its XXX Plenary.]*

B. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to

- Outline the principles involved in applying a risk-based approach to AML/CFT;
- Assist competent authorities and banks in the design and implementation of a risk-based approach to AML/CFT by providing examples of good practice; and
- Above all, support the development of a common understanding of what the risk-based approach to AML/CFT entails.

---

1 www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

2 Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector: www.fatf-gafi.org/documents/documents.jsp?lang=en.

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

C. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance addresses banking supervisors and practitioners in the banking sector[4].

6. It consists of three sections. Section I sets out the key elements of the risk-based approach and needs to be read in conjunction with Sections II and III, which provide specific guidance on the effective implementation of a RBA to banking supervisors (Section II) and banks[5] (Section III).

7. This Guidance recognises that an effective RBA will build on, and reflect, a country's legal and regulatory approach, the nature, diversity and maturity of its banking sector and its risk profile. It sets out what countries should consider when designing and implementing a RBA; but it does not override the purview of competent authorities.

8. This guidance paper is non-binding and even though compliance with it is not assessed in the FATF mutual evaluation or assessment process, countries, competent authorities and banks should consider taking into consideration its recommendations, which outline the main principles for applying an effective RBA to AML/CFT. This guidance paper should be read in conjunction with the FATF Recommendations, especially Recommendation 1 (R. 1) and its Interpretive Note (IN). It draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement the Recommendations.

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

A. WHAT IS THE RBA?

9. A RBA to AML/CFT means that countries, competent authorities, institutions and organisations are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

10. ML/TF risk is a function of three factors: threat (persons, object or activity with the potential to cause harm), vulnerability (things that may be exploited by the threat or that may support or facilitate its activities) and consequence (the impact or harm that may be caused)[6]. When assessing ML/TF risk, countries, institutions and organisations should analyse and seek to understand how the ML/TF risks they identified affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures.[7] The RBA is not a "no failures" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CTF risks, however an institution is used, unwittingly, for ML or TF purposes.

4 Banking activities includes the activities or operations described in the FATF Glossary under "Financial institutions", in particular 1., 2. and 5.

5 In this paper, the term 'bank' refers to credit institutions that carry out banking activities but may not necessarily be banks themselves.

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

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

11. A RBA does not exempt countries, institutions and organisations from assessing and, where appropriate, mitigating ML/TF risk where these risks are low.[8]

B. THE RATIONALE FOR A NEW APPROACH

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

13. One of the most important changes was the increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework.[9] This is an over-arching requirement applicable to all relevant FATF Recommendations.

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

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

C. APPLICATION OF THE RISK-BASED APPROACH

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

- 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 [11], countries should consider extending their regime to additional sectors or activities if they pose a higher risk of ML/TF, or consider exempting certain sectors or activities from some AML/CFT obligations where the ML/TF risks associated with those sectors or activities are low[12];

---

8 Where the ML/TF risks have been assessed as low, INR 1 allows countries not to apply some of the FATF Recommendations while INR10 allows the application of Simplified Due Diligence measures to take into account the nature of the lower risk – see INR 1 para 6, 11 and 12 and INR 10 para 16 and 21.

9 R. 1

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

11 See Glossary, definitions of Financial Institutions and Designated Non Financial Businesses and Professions

12 INR 1, paragraph 6

- How those subject to the AML/CFT regime should be supervised for compliance with this regime: AML/CFT supervisors should consider a bank's own risk assessment and mitigation, and acknowledge the degree of discretion allowed under the national RBA, while INR 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision; and

- How those subject to the AML/CFT regime should comply: where the ML/TF risk associated with a situation is higher, competent authorities and banks have to take enhanced measures to mitigate the higher risk. Conversely, where the ML/TF risk is lower, standard AML/CFT measures may be reduced.

D. CHALLENGES

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

Affording discretion to banks

18. 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. When implementing the RBA, countries must decide how much discretion should be afforded to financial institutions in terms of assessing to which risks they are exposed and how these risks should be mitigated. Banks' identification and assessment of ML/TF risk must take account of the national legal and regulatory framework, including any areas of prescribed risk and its mitigation, and consider national risk assessments in line with R. 1. Where ML/TF risks are increased, banks must always apply enhanced due diligence, although discretion might be allowed in the measures to be taken (e.g. varying the degree of enhanced ongoing monitoring)[13]. This does not take away the responsibility for banks to take reasonable measures to identify and understand fully the risks to which they are exposed.

19. Countries will have to consider carefully, inter alia, the capacity and AML/CFT expertise and experience of the banking sector and of their supervisory bodies when granting discretion to financial institutions[14]. Countries should also take into account evidence from competent authorities concerning the level of compliance in the banking sector, and the sector's culture in dealing with ML/TF risk. For example, where a country's financial services sector benefits from sufficient capacity and expertise, and has a good compliance culture, affording greater flexibility in the assessment and mitigation of ML/TF risk may be justified, as the banking sector should be better equipped to exercise discretion appropriately. In such cases, the supervisory bodies will also need sufficient expertise and resources to supervise the exercise of that discretion adequately. However, in countries where the financial services sector has low capacity and relatively little AML/CFT expertise, it might not be adequately equipped initially to effectively identify, assess and mitigate ML/TF risk thereby undermining the country's AML/CFT defences.[15] In such cases, a more prescriptive implementation of the RBA (for example, where competent authorities specify how particular risks are to be mitigated) may be appropriate until national AML/CFT expertise is strengthened[16].

---

13 R. 1

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

15 INR 1

16 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.

Identifying ML/TF risk

20. Access to accurate, timely and objective information about ML/TF risks is a prerequisite for an effective RBA. Where information is not readily available, for example where competent authorities have inadequate data to assess risks, are unable to or do not share important information (i.e. due to its sensitivity), on ML/TF risks and threats or where access to information is restricted by, for example, censorship or data protection provisions, banks will be unable to correctly identify (i.e. find and list) ML/TF risk and therefore fail to assess and mitigate it appropriately. Competent authorities are therefore encouraged to publish as much information as possible about ML and TF risks in order to assist banks.

[Note to FATF: In some instances, competent authorities may decide not to share important information to jurisdictions and entities, although they may have the legal ability to do so]

Assessing ML/TF risk

21. Assessing ML/TF risk means that countries, competent authorities and banks have to determine how the ML/TF threats identified will affect them. They must analyse the information obtained to understand the likelihood of these risks occurring and the impact that these would have if they did occur[17]. *[Note to FATF: "impact" should be defined – Does it relate to the impact on the national economy or just the impact on the entity?]*As a result of a risk assessment, ML/TF risks are often classified as low, medium and high, although other classifications are possible. This classification is meant to assist understanding ML/TF risks and to help prioritise them. Assessing ML/TF risk therefore goes beyond the mere collection of information: it forms the basis for effective ML/TF risk mitigation and must be kept up-to-date to ensure it remains relevant.

22. Assessing and understanding risks means that competent authorities and banks need to have skilled personnel and be technically equipped to carry out this work.

Mitigating ML/TF risk

23. The FATF Recommendations require that, when applying a RBA, banks and competent authorities decide on the most appropriate and effective way to mitigate the ML/TF risk they have identified. This implies that they should take enhanced measures to manage and mitigate situations in which the ML/TF risk is higher; and that, correspondingly, in lower risk situations, exemptions or simplified measures may be applied.[18]

24. Specific Recommendations set out in more detail how this general principle applies to particular requirements[19].

Developing a common understanding of the RBA

25. The effectiveness of a RBA depends on a common understanding by competent authorities and banks 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, banks have to deal

---

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

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

19 For example, R. 10 on Customer Due Diligence, R. 12 on Politically Exposed Persons, R. 13 on correspondent banking

with the risks they identify, and it is important that supervisors in particular issue guidance to banks on how they expect them to meet their legal and regulatory AML/CFT obligations in a risk-sensitive way. These measures should be supported by ongoing and effective communication between competent authorities and banks as an essential prerequisite for the successful implementation of a RBA.

26. It is important that competent authorities acknowledge that in a risk-based regime, not all banks will adopt identical AML/CFT controls and that a single isolated incident of crystallised risk may not necessarily invalidate the structure of a bank's AML/CFT controls. On the other hand, banks should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

Financial inclusion

27. A RBA may help foster financial inclusion. In applying a RBA, countries may establish specific cases for exemptions in the application of FATF Recommendations[20], or allow financial institutions to be more flexible in their application of CDD measures in case of lower ML/FT risks.

28. However, being potentially financially excluded does not automatically equate to low or lower ML/TF risk. Financial exclusion can have many reasons, including a poor credit rating or a customer's criminal background. ~~and I~~institutions should not, therefore, apply simplified due diligence measures or exemptions solely on the basis that the customer is financially excluded. There may be some occasions, where a financially excluded person may be subject to enhanced due diligence, for example, where that person has a criminal background involving offences of dishonesty.

SECTION II – GUIDANCE FOR SUPERVISORS

29. The RBA to AML/CFT aims to ensure that measures to mitigate ML/FT risk are commensurate to the risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that addresses the application of a risk-based approach by banks.

A. THE RISK-BASED APPROACH TO SUPERVISION

30. Recommendation 26 requires countries to ensure that banks are subject to adequate AML/CFT regulation and supervision. INR 26 requires supervisors to allocate supervisory resources to areas of higher

[20] As a general rule, R.10 does not allow financial institutions to keep anonymous accounts or accounts in obviously fictitious names. Nevertheless, paragraphs 2 and 6 of INR.1 provide that: "*Countries may also, in strictly limited circumstances and where there is a proven low risk of ML/TF, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP*"… and "*Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided: (a) there is a proven low risk of ML and TF; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP*" (para.6). This exemption has been implemented by different countries in the interest of financial inclusion policies. See also paragraphs 56 and 57 of the FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion on the main challenges for countries seeking to make use of the proven low risk exemption.

ML/TF risk, on the basis that supervisors understand the ML/TF risk in their country and have on-site and off-site access to all information relevant to determining a bank's risk profile.

Box 1 - Additional sources of information

Report by the European supervisory authorities

In October 2013, the European Supervisory Authorities (EIOPA for insurance and occupational pensions, EBA for banking and ESMA for securities) published a '*Preliminary report on anti-money laundering and counter financing of terrorism risk-based supervision*'. This report builds on the FATF Standards and sets out what the RBA to AML/CFT supervision entails. It also lists a series of self-assessment questions supervisors may ask themselves when reviewing their approach.

BCBS Guidelines

In January 2014, the Basel Committee on Banking Supervision published a set of guidelines to describe how banks should include the management of risks related to money laundering and financing of terrorism within their overall risk management framework, "*Sound management of risks related to money laundering and financing of terrorism*". These guidelines are intended to support the implementation of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation issued by the FATF in 2012. The FATF's present Guidance provides a general framework for the application of the RBA, by supervisors and the banking sector. More detailed guidelines on the implementation of the RBA by supervisors can be found in the BCBS document.

Understanding ML/TF risk

31. Supervisors need to understand the ML/TF risks to which the banking sector is exposed. They also need to understand the ML/TF risks associated with individual banks and banking groups.

32. Supervisors may need to draw on a variety of resources to identify and assess ML/TF risks.

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

34. For individual banks, supervisors will take into account the nature and complexity of the bank's products and services, delivery channels, customer profiles and countries of operations. Information drawn from prudential supervision or group-wide AML/CFT supervision, such as the bank's size, business model, quality of risk management, individual lines of business, oversight functions and the bank's other stakeholders such as other supervisors and law enforcement agencies may be helpful in determining the extent to which a bank is likely to effectively manage the ML/TF risk to which it is exposed.

35. Supervisors should review their assessment of both the sector's and banks' ML/TF risk profile periodically and in any case when a bank's circumstances change or relevant new threats emerge.

Examples of different ways banking supervisors assess ML/TF risk in the banking sector and in individual banks[21]

Mitigating ML/TF risk

36. The FATF Recommendations require supervisors to allocate proportionately more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual banks are exposed. It also means that where detailed supervision of all banks for AML/CFT purposes is not feasible, supervisors should ensure that they give priority to the areas of higher risk, either in the individual banks or to banks operating in a particular sector.

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

a) Adjusting the intensity of checks required to perform their authorisations function: supervisors can adjust the level of information they require when working to ensure that criminals or their associates do not hold a significant or controlling interest in a bank. For example, 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 thus supervisors may decide to base their approval decisions on a review of relevant documentation only. *[Note to FATF: consider the converse "Where example, the ML/TF risk associated with the sector is high, the opportunities for ML/TF associated with a particular business activity may be increased and thus supervisors may decide to base their approval decisions once additional measures have been undertaken such as commissioning an independent report from an accounting or law firm and conducting due diligence on the owners and those with management control of the entity."]*

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

c) Adjusting the frequency and nature of ongoing AML/CFT supervision: supervisors should adjust the frequency of AML/CFT supervision in line with the risks identified. Supervisors should stand prepared to combine periodic reviews with ad hoc AML/CFT supervision as issues emerge, e.g. as a result of whistleblowing, information from law enforcement, or other supervisory findings resulting from, for example, general prudential supervision or a bank's inclusion in thematic review samples.

Example of different ways banking supervisors adjust the frequency of ML/TF supervision in line with the risks identified[22]

d) Adjusting the intensity of AML/CFT supervision: supervisors should decide on the appropriate level of assessment in line with the risks identified. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the bank's CDD, reporting and record keeping policies and processes, interviews with operational staff and AML/CFT assessment in particular lines of business.

[21] It is considered to include references or links to national supervisory practices in this field.

[22] It is considered to include references or links to national supervisory practices in this field.

***Examples of different ways banking supervisors adjust the intensity of ML/TF supervision in line with the risks identified*[23]**

38. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and their AML/CFT rules and guidance remain adequate. ~~Whenever appropriate, and in compliance with relevant confidentiality requirements, T~~these findings should be communicated to banks to enable them to enhance their RBA.

39. In line with Recommendation 26 and the application of the Core Principles relevant for AML/CFT[24], banking supervisors should ensure that they consider the results of other prudential or financial supervision in their AML/CFT supervisory activities. Similarly, they should ensure that the broader prudential findings that drive the overall supervisory strategies of banks are informed by, and adequately address, the findings of the AML/CFT supervisory programme.

B. SUPERVISION OF THE RISK-BASED APPROACH

General approach

40. It is important that supervisors discharge their functions in a way that is conducive to banks' adoption of a risk-based approach. This means that supervisors have to take steps to ensure their staff are equipped to assess whether a bank's systems and controls are appropriate in view of the risks identified and the controls required. It also implies that supervisors should articulate and communicate clearly their expectations of the measures needed for banks to comply with the applicable legal and regulatory framework. The aim should be to ensure that supervisory actions are in most cases predictable, consistent and proportionate and to this end, training of supervisory staff and the effective communication of expectations to banks are key. Supervisors must ensure that, as far as possible, they assess a bank and its peers in a consistent manner and seek to avoid individual supervisory staff using individual interpretations when assessing a bank's AML and CTF controls

41. To support their understanding of the overall strength of measures in the banking sector, supervisors should be able to compare a bank's AML/CFT programme with those of the bank's peers to inform their judgment of the quality of the bank's controls. Supervisors should, however, note that under the RBA, there may be valid reasons why banks' controls differ: supervisors must be equipped to evaluate the merits of these differences. Supervisors should therefore recognise that it may not be appropriate, in all cases, for one bank to adopt certain controls which are used by that bank's peers.

42. Supervisors should understand the ML/TF risks faced by the sector and by the banks. They should, in particular, have a thorough understanding of higher and lower risk lines of business to ensure a sound judgment about the proportionality and adequacy of AML/CFT controls. Supervisors must engage in an open dialogue with individual banks about the supervisor's views on AML/CTF controls faced by that institution.

[23] It is considered to include references or links to national supervisory practices in this field.

[24] Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-11, 18, 21-23, and 25; and International Organization of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D (c. 26.4. in the 2013 Methodology).

43. The general principles outlined above in relation to domestic banks and domestic banking groups also apply to international banking groups. The application is, however, more complex as it involves legal frameworks and risks of more than one jurisdiction and also supervision by more than one national supervisory body. The BCBS's "Sound management of risks related to money laundering and financing of terrorism" contains more information.[25]

Training

44. INR 26 provides that supervisors who supervise banks, in their implementation of a risk-based approach, should understand the degree of discretion a bank has in assessing and mitigating its ML/TF risks. In particular, supervisors should ensure staff are able to assess the quality of a bank's ML/TF risk assessments and to consider the adequacy and effectiveness of the bank's AML/CFT policies, procedures and internal controls in light of this risk assessment.

45. Training should allow supervisory staff to form sound judgments about the adequacy and proportionality of a bank's AML/CFT controls.

Guidance

46. Supervisors should communicate their expectations of banks' compliance with their legal and regulatory obligations.[26] This may be in the form of high-level requirements based on desired outcomes, risk-based rules, information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Supervisors should also consider issuing guidance to banks on how to comply with their legal and regulatory AML/CFT obligations in a way that fosters financial inclusion. Supervisors should ensure that their guidance covers all products and services offered by banks. Supervisors should recognise that individual banks may elect, in particular cases, not to follow any issued guidance. This departure should be justified by the bank and soundly assesses by the supervisor.

47. Where supervisors' guidance remains high-level and principles-based, guidance written by industry sectors on how to meet the legal and regulatory obligations may gain more importance. Banks should note, however, that the private sector guidance they take into consideration must be consistent with the international standards adopted by countries and guidelines issued by competent authorities.

Examples of different approaches to banking supervisory guidance[27]

48. Supervisors should liaise with other relevant domestic supervisory authorities to ensure a coherent interpretation of the legal obligations and to minimise disparities. This is particularly important where more than one supervisor is responsible for AML/CFT supervision (for example, where the prudential supervisor and the AML/CFT enforcement authorities are in different agencies). Multiple guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among banks.

[25] Part IV. See also BCBS *Good Practice Principles on Supervisory Colleges* (2010); BCBS *Revised Good Practice Principles on Supervisory Colleges* (Consultative document) (2014) on collaboration and exchanges of information between home and host supervisors.

[26] R. 34

[27] It is considered to include references or links to national supervisory practices in this field.

SECTION III – GUIDANCE FOR BANKS[28]

49. The RBA to AML/CFT aims to ensure that measures to mitigate -ML/FT risk are commensurate to the risks identified. In the case of banks, this applies to the way banks organise their internal controls and implement policies and procedures to deter and detect ML/TF, including, where relevant, at group level.

50. Banking encompasses a wide range of financial products and services, which are associated with different ML/TF risks. These include, but are not limited to:

- *Retail banking*, where banks offer products and services directly to personal and business customers (including legal arrangements), such as current accounts, loans (including mortgages) and savings products;
- *Corporate and investment banking*, where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions; and
- ~~*Investment services*~~*Wealth management*, where banks provide products and services to manage their customers' wealth (sometimes referred to as private banking).

51. Banks should be mindful of those differences when assessing and mitigating the ML/TF risk to which they are exposed. Supervisors should be mindful that in some financial products and services that individual banks will utilise the services or facilities of other AML/CTF regulated institutions. In such circumstances, banks may choose to rely on public sector evaluations of the quality or effectiveness of the jurisdiction in which the AML/CTF regulated institution is based. In order to assist banks allocate their resources to the higher risks, supervisors should publish lists of jurisdictions and financial products or services which the supervisor assesses to present a higher risk.

A. INTERNAL CONTROLS

52. Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, controls to ensure and monitor the integrity of staff in accordance with the applicable local legislation, compliance and controls to test the overall effectiveness of the bank's policies and processes to identify, assess and monitor risk.

53. For larger banking groups, there should be controls in place to ensure a consistent approach to AML/CFT controls across the group. The BCBS's *"Sound management of risk related to money laundering and financing of terrorism"* document[29] provides comprehensive guidance to banks on the effective management of ML/TF risk in a group-wide and cross-border context. It explains the rationale behind and principles of consolidated risk management; how group-wide AML/CFT policies and procedures should be consistently applied and supervised across the group, and, where reflecting local business considerations and the requirements of the host jurisdiction, should still be consistent with and

[28] In this paper, the term 'bank' refers to credit institutions that carry out banking activities but may not necessarily be banks themselves.

[29] See part III

supportive of the broader policies and procedures of the group; how banks should address differences in home/host requirements. Importantly, it also provides detail on how banks that are part of a group should share information with members of the same group with a view to informing and strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.

Risk assessment

54. The risk assessment forms the basis of a bank's RBA. It is designed to enable the bank to understand how, and to what extent, it is vulnerable to ML/TF. It will often result in a stylised categorisation of risk, which will help banks determine the level of AML/CFT resources necessary to mitigate that risk. It should always be properly documented, maintained and communicated to relevant personnel within the bank.

55. A bank's risk assessment need not be complex, but should be commensurate with the nature and size of the bank's business. For smaller or less complex banks, (for example where the bank's customers fall into similar categories and/or where the range of products and services the bank offers are very limited), a simple risk assessment might suffice. Conversely, where the bank's products and services are more complex, where there are multiple subsidiaries or branches offering a wide variety of products, and/or their customer base is more diverse, a more sophisticated risk assessment process will be required.

56. In identifying and assessing the ML/TF risk to which they are exposed, banks should consider a range of factors which may include:

- The nature, scale, diversity and complexity of their business;
- Their target markets and whether they include a significant number of customers identified as high risk;
- ~~The number of customers already identified as high risk;~~
- The jurisdictions the bank is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption, organised crime and/or deficient AML/CFT controls as assessed by recognised independent institutions;
- The involvement of other AML/CTF regulated institutions in the transaction or payment flow;
- The distribution channels, including the extent to which the bank deals directly with the customer or the extent to which it relies (or is allowed to rely on) third parties to conduct CDD; and
- The volume and size of its transactions considering the usual activity of the bank and the profile of its customers.[30]

57. Banks should complement this information with information obtained from relevant internal and external sources, such as heads of business, relationship managers, national risk assessments, lists issued by inter-governmental international organisations and national governments, AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies. Banks may elect to, if they wish, to rely on national risk assessments and lists issued by inter-governmental international organisations and national governments, AML/CTF evaluations and follow up reports by FATF or

[30] INR 1 and 10

associated assessment bodies.-They should review their assessment periodically and in any case when their circumstances change or relevant new threats emerge.

Box 2

Examples of ML/TF risk associated with different banking activities[31]:

- Retail banking: provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services
- Wealth management: culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions
- Investment banking: layering and integration; transfer of assets between parties in exchange for cash or other assets;*[Note for FATF: these features are not specific to investment banking]* reliance on other institutions regulated for AML/CTF purposes in the transaction flow; global nature of markets
- Correspondent banking: high value transactions, limited information about the remitter and source of funds, the possibility that PEPs are involved regarding the ownership of a bank, reliance on other institutions regulated for AML/CTF purposes

58. The risk assessment should be approved by senior management and form the basis for the development of policies and procedures to mitigate ML/TF risk. It should be reviewed and updated on a regular basis.

Governance

59. The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the bank.

60. Senior management should:

- create a culture of compliance where ML/TF is not acceptable: senior management should send a clear message that the bank will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks;
- implement adequate mechanisms of internal communication related to the actual or potential ML/FT risks faced by the bank. These mechanisms must link the board of directors, the AML/CFT ~~chief~~compliance officer, the IT division and each of the business areas; set and enforce the bank's risk appetite: senior management should decide on the extent of measures needed to mitigate the level of ML/TF risk identified; and *[Note for FATF; please clarify why the IT division is included – please clarify how a risk appetite may be defined – is it that a certain percentage of business or customers may be higher risk]*

[31] The proposed categorisation of banking activities is purely indicative (see par. 46) and the list of identified risks is illustrative and non-exhaustive.

- ensure that the bank's AML/CFT unit is adequately resourced.

Box 3

Examples of steps taken by banks' senior management to create a culture of compliance

– staff surveys;

- acknowledgement within the bank of staff who turn down profitable business due to ML/TF concerns;

- reward structures that are not excessively based on profit or revenue generation;

- public reporting of ethics code compliance;

- senior management approval of high risk relationships;

- senior management involvement in AML/CTF training of staff;

- senior management refusal of high-risk business relationships

61. This implies that senior management must not only know about the ML/TF risks to which the bank is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. Senior management should therefore ensure that:

- it receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the bank is exposed through its activities and individual business relationships;
- it receives sufficient and objective information to understand whether the bank's AML/CFT controls are effective (for example information from the ~~Chief~~AML/CTF c~~C~~ompliance ~~O~~officer on the effectiveness of control, suggested improvements in control procedures or audit reports);
- processes are in place to escalate important decisions that directly impact the ability of the bank to address and control risks.

Box 4

Examples of good MI routinely provided to senior management that supports their AML/CFT role, including reports of compliance initiatives, compliance failure and corrective actions, number and nature of STRs, overview of high risk customers.

62. It is important that responsibility for the consistency and effectiveness of AML/CFT controls be clearly allocated to an individual of sufficient seniority within the bank to signal the importance of ML/TF risk management and compliance, and to ensure that ML/TF issues are brought to senior management's attention. This includes, but is not restricted to, the appointment of a compliance officer at management level[32].

[32] INR 18

Ensuring and monitoring compliance

63. A bank's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

Vetting, recruitment and remuneration

64. Banks should take reasonable measures to ensure, in accordance with applicable local legislation, that staff they employ have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls.

65. The level of vetting of individual staff members should not solely depend on his/her management role within the bank but also on ~~reflect~~ the ML/TF risks to which the bank is ~~individual staff are~~ exposed. ~~and not focus merely on senior management roles~~. Banks should also have processes in place to monitor an individual's integrity or suitability for the position they occupy and take steps to ensure that performance-related payments take into account how effective they are at implementing control, and not based solely on the generation of profit or revenue. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities, such as the monitoring of customer activity, especially if they are also involved ~~with~~in or report to the business/ profit generating areas of the institution.

Box 5

Example: vetting/screening policies, conflict of interest policies. Situations where conflicts of interest might affect AML/CFT performance, e.g. relationship managers in banks that become too close to their customers to be objective

Training and awareness

66. The effective application of AML/CFT policies and procedures depends on staff within banks understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate. It is therefore important that bank staff receive AML/CFT training, which should be:

- Of high quality, relevant to the bank's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
- Obligatory for all relevant staff;
- Tailored to particular lines of business within the bank, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks;
- Effective: banks should be able to satisfy themselves that training has the desired effect, for example by requiring staff to pass tests or by monitoring levels of compliance with the bank's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;

- Ongoing: in line with INR 18, AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired;

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

67. Overall, the training should also seek to build up a culture of compliance amongst the bank's staff.

Assessment of controls

68. Banks should take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. To this end, their controls should be monitored on an ongoing basis by the bank's AML/CTF compliance officer. In addition, the adequacy of and compliance with banks' AML/CFT controls should be reviewed by an internal or external auditor.

69. ~~Recommendation~~INR 18 requires countries to require banks to appoint an AML/CTF compliance officer at management level. In addition to advising relevant staff how to meet their obligations, their role should be to monitor and assess ML/TF risks across the bank as well as the adequacy and effectiveness of the measures the bank has put in place to mitigate the risks. The compliance officer should therefore have the necessary independence, authority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including all records across all lines of business~~,~~ and across all foreign branches and subsidiaries).

Box 6

Examples: ways to ensure compliance, e.g. mechanisms to allow staff to report areas of policy or controls they find unclear / unhelpful / ineffective. Sources of information that support the compliance officer's / auditor's view of the adequacy of the bank's controls, e.g. training pass rates, compliance failures, whistleblowing information, analysis of questions received from staff

70. ~~Recommendation~~INR 18 also requires countries to require banks to have an independent audit function to test the bank's AML/CFT programme with a view to establishing the effectiveness of the bank's overall AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. This independent audit function may be performed by the bank's internal audit department, where one exists. The findings should inform senior management's view of the design and implementation of the bank's AML/CFT framework. The audit function needs to examine the adequacy of all risk determinations and should therefore not focus exclusively on higher risks.

71. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or any whistleblowing hotlines that the bank may operate.

B. DETERRING ML/TF: IDENTIFICATION, VERIFICATION AND THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

72. Banks should develop and implement policies and procedures to mitigate the ML/TF risks they have identified through their individual risk assessment. Customer due diligence (CDD) processes should

be designed to help banks understand who their customers are by requiring them to gather information on what they do and why they require particular banking services. The initial stages of the CDD process should be designed to help banks assess the ML/TF risk associated with a proposed business relationship and deter persons from establishing a business relationship to conduct illicit activity.

73. Based on a holistic view of the information obtained in the context of their application of CDD measures, banks will be able to prepare a complete customer risk profile. This will determine the level and type of ongoing monitoring and support the bank's decision whether to enter into, or continue, the business relationship. Risk profiles can apply at the individual customer level or, where groups of customers display homogenous characteristics (for example, clients with similar income range, or conducting similar types of banking transactions) can be applied to such groups. This approach is particularly relevant for retail banking customers.

74. Initial CDD comprises:

- Identifying the customer and, where applicable, the customer's beneficial owner;
- Verifying the customer's identity on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; and
- Understanding the purpose and intended nature of the business relationship and, where appropriate, obtaining further information, such as the source of funds or the source of wealth.

75. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed above under Risk Assessment. This means that the amount and type of information obtained, and the extent to which this information is verified, may need to be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business relationship is lower. Banks therefore have to draw up individual customer risk profiles[33], which serve to help banks apply the appropriate level of CDD.

Box 7

Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR 10):

- EDD
  - ✓ obtaining additional identity information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
  - ✓ carrying out –adverse media searches and using the information to inform the individual customer risk assessment
  - ✓ commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity
  - ✓ verifying the source of funds or wealth involved in the business relationship to be satisfied

[33] based on the bank's own risk assessment and taking into account risk factors such as those outlined in the FATF standards, e.g. in INR 10 and Recommendations / INR 12-16.

that they do not constitute the proceeds from crime

- ✓ seeking additional information from the customer about the purpose and intended nature of the business relationship.

- SDD:

  - ✓ obtaining less information, and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship;

  - ✓ postponing the verification of the customer's identity

Box 8

CDD and financial inclusion considerations

The application of a RBA to CDD may support financial inclusion objectives by providing for a more flexible application of CDD measures to certain categories of customers who might otherwise struggle to meet banks' CDD requirements. However, financial exclusion in itself is not an indicator of low ML/TF risk and banks have to take an informed decision, based on a holistic assessment of ML/TF risk, whether exemptions or SDD measures may be appropriate.

76. Where banks cannot apply the appropriate level of CDD, R. 10 requires that banks do not enter into the business relationship or terminate the business relationship.

77. The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* provides detailed guidance to banks on the management of money laundering risk in correspondent banking and in situations where banks rely on third parties to carry out all, or part, of their CDD.

C. MONITORING AND REPORTING

Ongoing CDD/Monitoring

78. Ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the business relationship. Monitoring also involves identifying changes to the customer profile, and keeping it up to date, which may require the application of new, or additional, CDD measures. Monitoring transactions is an essential base component in identifying transactions that are potentially suspicious.

79. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules and ensure they address the identified ML/TF risks.

80. Banks should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring will be required for higher risk situations, while banks may decide to reduce the frequency and intensity of monitoring where the risks are lower. The adequacy of monitoring systems and the factors leading banks to adjust the level of monitoring should be reviewed regularly to ensure their continued relevance to the bank's AML/CFT risk programme.

Box 9

Examples:

- Monitoring in high risk situations (e.g. daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds etc)

- Monitoring in lower risk situations (e.g. thresholds, low frequency, automated systems)

The BCBS's guidance on the *Sound management of risk related to money laundering and financing of terrorism* sets out in Section II 1 (d) what banks should consider when assessing whether their monitoring system is adequate. It stresses that a bank should have a monitoring system in place that is adequate with respect to its size, its activities and complexity as well as the risks present in the bank. For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process.

81. To this end, banks should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

Reporting

82. Recommendation 20 requires countries to ensure that if a bank suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions promptly to the relevant FIU. Therefore banks should ensure they have the ability to flag unusual movement of funds or transactions for further analysis. Banks should have appropriate case management systems to ensure that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious.

83. Funds or transactions that are suspicious must be reported promptly to the FIU and in the manner specified by competent authorities. The processes banks put in place to escalate suspicions and, ultimately, report to the FIU, need to reflect this.