Enero 2014

SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM

AUTOR: BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-403-9 (online)

Contents

Sound management of risks related to money laundering and financing of terrorism 1

I. Introduction 1

II. Essential elements of sound ML/FT risk management 4

1. Assessment, understanding, management and mitigation of risks 4

(a) Assessment and understanding of risks 4

(b) Proper governance arrangements 4

(c) The three lines of defence 5

(d) Adequate transaction monitoring system 6

2. Customer acceptance policy 7

3. Customer and beneficial owner identification, verification and risk profiling 8

4. Ongoing monitoring 10

5. Management of information 11

(a) Record-keeping 11

(b) Updating of information 11

(c) Supplying information to the supervisors 12

6. Reporting of suspicious transactions and asset freezing 12

(a) Reporting of suspicious transactions 12

(b) Asset freezing 12

III. AML/CFT in a group-wide and cross-border context 13

1. Global process for managing customer risks 13

2. Risk assessment and management 14

3. Consolidated AML/CFT policies and procedures 14

4. Group-wide information-sharing 15

5. Mixed financial groups 16

IV. The role of supervisors 16

Annex 1 20

Annex 2 24

Annex 3 33

Annex 4 34

Annex 5 45

Sound management of risks related to money laundering and financing of terrorism

I. Introduction

1. Being aware of the risks incurred by banks of being used, intentionally or unintentionally, for criminal activities, the Basel Committee on Banking Supervision is issuing these guidelines to describe how banks should include money laundering (ML) and financing of terrorism (FT) risks within their overall risk management.

2. The Committee has a long-standing commitment to promote the implementation of sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures that are critical in protecting the safety and soundness of banks and the integrity of the international financial system. Following an initial statement in 1988,[1] it has published several documents in support of this commitment. In September 2012, the Committee reaffirmed its stance by publishing the revised version of the *Core principles for effective banking supervision*, in which a dedicated principle (BCP 29) deals with the abuse of financial services.

3. The Committee supports the adoption of the standards issued by the Financial Action Task Force (FATF).[2] In February 2012, the FATF released a revised version of the *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (the FATF standards), to which the Committee provided input.[3] In March 2013, the FATF also issued *Financial Inclusion Guidance*, which has also been considered by the Committee in drafting these guidelines. The Committee's intention in issuing this paper is to support national implementation of the FATF standards by exploring complementary areas and leveraging the expertise of both organisations. These guidelines embody both the FATF standards and the Basel Core Principles for banks operating across borders and fits into the overall framework of banking supervision. Therefore, these guidelines are intended to be consistent with and to supplement the goals and objectives of the FATF standards, and in no way should they be interpreted as modifying the FATF standards, either by strengthening or weakening them.

4. In some instances, the Committee has included cross-references to FATF standards in this document in order to assist banks in complying with national requirements based on the implementation of those standards. However, as the Committee's intention is not to simply duplicate the existing FATF standards, cross-references are not included as a matter of routine.

5. The Committee's commitment to combating money laundering and the financing of terrorism is fully aligned with its mandate "to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability".[4] Sound ML/FT risk management has particular relevance

[1] See BCBS, *Prevention of criminal use of the banking system for the purpose of money-laundering*, December 1988, accessible at www.bis.org/publ/bcbsc137.pdf.

[2] The FATF is an intergovernmental body that develops international standards 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 defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin. The FATF works in close cooperation with other entities involved in this area, and in particular FATF associate members and observers. The Committee has observer status within the FATF.

[3] Annex 3 contains an excerpt of the most relevant FATF Recommendations that banks and supervisors should comply with when implementing their AML/CFT measures. This is not exhaustive and other FATF Recommendations, including the Interpretive Notes, may be relevant. The full document is accessible at www.fatf-gafi.org/recommendations.

[4] See Basel Committee on Banking Supervision, *Charter*, June 2018, accessible at www.bis.org/bcbs/charter.htm.

to the overall safety and soundness of banks and of the banking system, the primary objective for banking supervision, in that:

- it helps protect the reputation of both banks and national banking systems by preventing and deterring the use of banks to launder illicit proceeds or to raise or move funds in support of terrorism; and
- it preserves the integrity of the international financial system as well as the work of governments in addressing corruption and in combating the financing of terrorism.

6 The inadequacy or absence of sound ML/FT risk management exposes banks to serious risks, especially reputational, operational, compliance and concentration risks. Recent developments, including robust enforcement actions taken by regulators and the corresponding direct and indirect costs incurred by banks due to their lack of diligence in applying appropriate risk management policies, procedures and controls, have highlighted those risks. These costs and damage could probably have been avoided had the banks maintained effective risk-based AML/CFT policies and procedures.

7. It is worth noting that all these risks are interrelated. However, in addition to incurring fines and sanctions by regulators, any one of them could result in significant financial costs to banks (eg through the termination of wholesale funding and facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the diversion of limited and valuable management time and operational resources to resolve problems.

8. Consequently, this paper should be read in conjunction with a number of related Committee papers, including the following:

- *Core principles for effective banking supervision*, September 2012[5]
- *The internal audit function in banks*, June 2012[6]
- *Principles for the sound management of operational risk*, June 2011[7]
- *Corporate governance principles for banks,* July 2015[8]
- *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, May 2009[9]
- *Compliance and the compliance function in banks*, April 2005[10]
- *Principles for effective supervisory colleges*, June 2014[11]

9. In an effort to rationalise the Committee's publications on AML/CFT guidance, this document merges and supersedes two of the Committee's previous publications dealing with related topics: *Customer due diligence for banks*, October 2001 and *Consolidated KYC risk management*, October 2004. In updating these papers, the Committee has also increased its focus on risks associated with the usage by banks of third parties to introduce business (see Annex 1) and the provision of correspondent banking

5 Accessible at: www.bis.org/publ/bcbs230.pdf.

6 Accessible at: www.bis.org/publ/bcbs223.pdf.

7 Accessible at: www.bis.org/publ/bcbs195.pdf.

8 Accessible at: https://www.bis.org/bcbs/publ/d328.pdf.

9 Accessible at: www.bis.org/publ/bcbs154.pdf.

10 Accessible at: www.bis.org/publ/bcbs113.pdf.

11 Accessible at: https://www.bis.org/publ/bcbs287.pdf.

services (see Annex 2). Despite their importance and relevance, other specific risk areas such as politically exposed persons (PEPs), private banking and specific legal structures that were addressed in the previous papers have not been specifically developed in this guidance, since they are the subject of existing FATF publications.[12] In February 2016, this document was revised with a general guide to account opening (see Annex 4). Revisions to Annexes 2 (Correspondent banking) and 4 (General guide to account opening) issued in June 2017 guide the banks in the application of the risk-based approach for correspondent banking relationships, recognising that not all correspondent banking relationships bear the same level of risk and including an updated list of risk indicators that correspondent banks should consider in their risk assessment.

10. With respect to the scope of application, these guidelines should be read in conjunction with other standards and guidelines produced by the Committee that promote supervision of banking groups on a consolidated level.[13] This is particularly relevant in the context of AML/CFT since customers frequently have multiple relationships and/or accounts with the same banking group, but in offices located in different countries.

11. These guidelines are applicable to all banks. Some of the requirements may require adaptation for use by small or specialised institutions, to fit their specific size or business models. However, it is beyond the scope of this guidance document to address these adjustments.

12. These guidelines specifically target banks, banking groups (Parts II and III respectively) and banking supervisors (Part IV). As stated in BCP 29, the Committee is aware of the variety of national arrangements that exist for ensuring AML/CFT compliance, particularly the sharing of supervisory functions between banking supervisors and other authorities such as financial intelligence units (FIUs).[14] Therefore, for the purpose of these guidelines, the term "supervisor" might refer to these authorities. In jurisdictions where AML/CFT supervisory authority is shared, the banking supervisor cooperates with other authorities to seek adherence to these guidelines. Revisions to the guidelines in July 2020 provide detailed guidelines to enhance effective cooperation and information exchange between prudential and AML/CFT supervisors for banks in the domestic and cross-border context (paragraph 96 in Part IV and Annex 5). For the purpose of Annex 5, considering the jurisdictional diversity in institutional arrangements for allocating prudential and AML/CFT responsibilities and the importance of cooperation between the two supervisory functions regardless of institutional arrangements, the supervisory function that is generally responsible for prudential banking supervision is defined as the "prudential supervisor". Conversely, the supervisory function that is responsible for AML/CFT supervision is defined as the "AML/CFT supervisor". It also underlines the importance of cooperation with third parties (eg law enforcement agencies or FIUs).

13. It should be noted that the FATF standards that require countries to apply other measures in their financial sectors and other designated non-financial sectors, or establishing powers and responsibilities for the competent authorities, are not dealt with in this document.

[12] See in particular the *FATF Guidance on Politically Exposed Persons* (recommendations 12 and 22), accessible at www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

[13] See for example BCP 12 in *Core principles for effective banking supervision*, September 2012.

[14] Financial intelligence units are described in Recommendation 26 in the FATF Standards.

II. Essential elements of sound ML/FT risk management

14. In accordance with the updated *Core principles for effective banking supervision* (2012), all banks should be required to "have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities".[15] This requirement is to be seen as a specific part of banks' general obligation to have sound risk management programmes in place to address all kinds of risks, including ML and FT risks. "Adequate policies and processes" in this context requires the implementation of other measures in addition to effective CDD rules. These measures should also be proportional and risk-based, informed by banks' own risk assessment of ML/FT risks. This document sets out guidance in respect of such measures. In addition, other guidelines (see paragraph 8 above) are applicable or supplementary where no specific AML/CFT guidance exists.

1. Assessment, understanding, management and mitigation of risks

(a) Assessment and understanding of risks

15. Sound risk management[16] requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country,[17] sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied. The policies and procedures for CDD, customer acceptance, customer identification and monitoring of the business relationship and operations (product and service offered) will then have to take into account the risk assessment and the bank's resulting risk profile. A bank should have appropriate mechanisms to document and provide risk assessment information to competent authorities such as supervisors.

16. A bank should develop a thorough understanding of the inherent ML/FT risks present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business. This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information such as national risk assessments and country reports from international organisations. Policies and procedures for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control those identified inherent risks. Any resulting residual risk should be managed in line with the bank's risk profile established through its risk assessment. This assessment and understanding should be able to be demonstrated as required by, and should be acceptable to, the bank's supervisor.

(b) Proper governance arrangements

17. Effective ML/FT risk management requires proper governance arrangements as described in relevant previous publications of the Committee.[18] In particular, the requirement for the board of directors to approve and oversee the policies for risk, risk management and compliance is fully relevant in the

[15] See BCP 29 in *Core principles for effective banking supervision*, September 2012.

[16] See in particular BCP 15 in *Core principles for effective banking supervision*, September 2012 as well as Principle 6 in *Corporate governance principles for banks*, July 2015.

[17] Where appropriate, AML/CFT risk assessments at a supranational level should be taken into account.

[18] See, in particular, *The internal audit function in banks*, June 2012; *Corporate governance principles for banks*, July 2015; *Compliance and the compliance function in banks*, April 2005.

context of ML/FT risk. The board of directors should have a clear understanding of ML/FT risks. Information about ML/FT risk assessment should be communicated to the board in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions.

18. Explicit responsibility should be allocated by the board of directors effectively taking into consideration the governance structure of the bank for ensuring that the bank's policies and procedures are managed effectively. The board of directors and senior management should appoint an appropriately qualified chief AML/CFT officer to have overall responsibility for the AML/CFT function with the stature and the necessary authority within the bank such that issues raised by this senior officer receive the necessary attention from the board, senior management and business lines.

(c) The three lines of defence

19. As a general rule and in the context of AML/CFT, the business units (eg front office, customer-facing activity) are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. The second line of defence includes the chief officer in charge of AML/CFT, the compliance function but also human resources or technology. The third line of defence is ensured by the internal audit function.

20. As part of **the first line of defence**, policies and procedures should be clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the bank in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions.

21. A bank should have adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards. All banks should implement ongoing employee training programmes so that bank staff are adequately trained to implement the bank's AML/CFT policies and procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank according to their needs and the bank's risk profile. Training needs will vary depending on staff functions and job responsibilities and length of service with the bank. Training course organisation and materials should be tailored to an employee's specific responsibility or function to ensure that the employee has sufficient knowledge and information to effectively implement the bank's AML/CFT policies and procedures. New employees should be required to attend training as soon as possible after being hired, for the same reasons. Refresher training should be provided to ensure that staff are reminded of their obligations and their knowledge and expertise are kept up to date. The scope and frequency of such training should be tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the bank.

22. As part of **the second line of defence**, the chief officer in charge of AML/CFT should have the responsibility for ongoing monitoring of the fulfilment of all AML/CFT duties by the bank. This implies sample testing of compliance and review of exception reports to alert senior management or the board of directors if it is believed management is failing to address AML/CFT procedures in a responsible manner. The chief AML/CFT officer should be the contact point regarding all AML/CFT issues for internal and external authorities, including supervisory authorities or financial intelligence units (FIUs).

23. The business interests of a bank should in no way be opposed to the effective discharge of the above-mentioned responsibilities of the chief AML/CFT officer. Regardless of the bank's size or its management structure, potential conflicts of interest should be avoided. Therefore, to enable unbiased judgments and facilitate impartial advice to management, the chief AML/CFT officer should, for example, not have business line responsibilities and should not be entrusted with responsibilities in the context of data protection or the function of internal audit. Where any conflicts between business lines and the responsibilities of the chief AML/CFT officer arise, procedures should be in place to ensure AML/CFT concerns are objectively considered at the highest level.

24. The chief AML/CFT officer may also perform the function of the chief risk officer or the chief compliance officer or equivalent. He/she should have a direct reporting line to senior management or the board. In case of a separation of duties the relationship between the aforementioned chief officers and their respective roles must be clearly defined and understood.

25. The chief AML/CFT officer should also have the responsibility for reporting suspicious transactions. The chief AML/CFT officer should be provided with sufficient resources to execute all responsibilities effectively and play a central and proactive role in the bank's AML/CFT regime. In order to do so, he/she must be fully conversant with the bank's AML/CFT regime, its statutory and regulatory requirements and the ML/FT risks arising from the business.

26. **Internal audit, the third line of defence,** plays an important role in independently evaluating the risk management and controls, and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures. A bank should establish policies for conducting audits of (i) the adequacy of the bank's AML/CFT policies and procedures in addressing identified risks, (ii) the effectiveness of bank staff in implementing the bank's policies and procedures; (iii) the effectiveness of compliance oversight and quality control including parameters of criteria for automatic alerts; and (iv) the effectiveness of the bank's training of relevant personnel. Senior management should ensure that audit functions are allocated staff that are knowledgeable and have the appropriate expertise to conduct such audits. Management should also ensure that the audit scope and methodology are appropriate for the bank's risk profile and that the frequency of such audits is also based on risk. Periodically, internal auditors should conduct AML/CFT audits on a bank-wide basis. In addition, internal auditors should be proactive in following up their findings and recommendations.[19] As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate, subject to any prescribed auditing requirements applicable to AML/CFT measures.

27. In many countries, **external auditors** also have an important role to play in evaluating banks' internal controls and procedures in the course of their financial audits, and in confirming that they are compliant with AML/CFT regulations and supervisory practice. In cases where a bank uses external auditors to evaluate the effectiveness of AML/CFT policies and procedures, it should ensure that the scope of the audit is adequate to address the bank's risks and that the auditors assigned to the engagement have the requisite expertise and experience. A bank should also ensure that it exercises appropriate oversight of such engagements.

(d) Adequate transaction monitoring system

28 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. When a bank has the opinion that an IT monitoring system is not necessary in its specific situation, it should document its decision and be able to demonstrate to its supervisor or external auditors that it has in place an effective alternative. When an IT system is used, it should cover all accounts of the bank's customers and transactions for the benefit of, or by order of, those customers. It must enable the bank to undergo trend analysis of transaction activity and to identify unusual business relationships and transactions in order to prevent ML or FT.

29. In particular, this system should be able to provide accurate information for senior management relating to several key aspects, including changes in the transactional profile of customers. In compiling the customer's profile, the bank should incorporate the updated, comprehensive and accurate CDD information provided to it by the customer. The IT system should allow the bank, and where appropriate the group, to gain a centralised knowledge of information (ie organised by customer, product, across

[19] See BCBS, *The internal audit function in banks*, June 2012.

group entities, transactions carried out during a certain timeframe etc). Without being requested to have a unique customer file, banks should be able to risk-rate customers and manage alerts with all the relevant information at their disposal. An IT monitoring system must use adequate parameters based on the national and international experience on the methods and the prevention of ML or FT. A bank may make use of the standard parameters provided by the developer of the IT monitoring system; however, the parameters used must reflect and take into account the bank's own risk situation.

30. The IT monitoring system should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report (STR) or taking other steps in order to minimise the risk. The chief AML/CFT officer should have access to and benefit from the IT system as far as it is relevant for his/her function (even if operated or used by other business lines). Parameters of the IT system should allow for generation of alerts of unusual transactions and should then be subject to further assessment by the chief AML/CFT officer. Any risk criteria used in this context should be adequate with regard to the risk assessment of the bank.

31. Internal audit should also evaluate the IT system to ensure that it is appropriate and used effectively by the first and second lines of defence.

2. Customer acceptance policy

32. A bank should develop and implement clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment.[20] When assessing risk, a bank should consider the factors relevant to the situation, such as a customer's background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence (when different), products used, nature and purpose of accounts, linked accounts, business activities and other customer-oriented risk indicators in determining what is the level of overall risk and the appropriate measures to be applied to manage those risks.

33. Such policies and procedures should require basic due diligence for all customers and commensurate due diligence as the level of risk associated with the customer varies. For proven lower risk situations, simplified measures may be permitted, if this is allowed by law. For example, the application of basic account-opening procedures may be appropriate for an individual who expects to maintain a small account balance and use it to conduct routine retail banking transactions. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. The FATF *Financial Inclusion Guidance*[21] provides useful guidelines on designing AML/CFT procedures that are not overly restrictive to the financially or socially disadvantaged.

34. Where the risks are higher, banks should take enhanced measures to mitigate and manage those risks. Enhanced due diligence may be essential for an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or an individual who is a politically exposed person (PEP). In particular, such enhanced due diligence is required for foreign PEPs. Decisions to enter into or pursue business relationships with higher-risk customers should require the application of enhanced due diligence measures, such as approval to enter into or continue such relationships, being

[20] The FATF standards also include useful guidelines on how the bank may effectively implement a risk-based approach (see in particular Recommendation 1).

[21] See FATF, *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion*, February 2013, accessible at http://www.fatf-gafi.org/topics/financialinclusion/.

taken by senior management. The bank's customer acceptance policy should also define circumstances under which the bank would not accept a new business relationship or would terminate an existing one.

3. Customer and beneficial owner identification, verification and risk profiling

35. For the purposes of this guidance, a customer refers, in accordance with the FATF Recommendation 10, to any person[22] who enters into a business relationship or carries out an occasional financial transaction with the bank. The customer due diligence should be applied not only to customers but also to persons acting on their behalf and beneficial owners.[23] In accordance with the FATF standards, banks should identify customers and verify their identity.[24]

36. A bank should establish a systematic procedure for identifying and verifying its customers and, where applicable, any person acting on their behalf and any beneficial owner(s). Generally, a bank should not establish a banking relationship, or carry out any transactions, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. Consistent with BCP 29[25] and the FATF standards, the procedures should also include the taking of reasonable measures to verify the identity of the beneficial owner. A bank should also verify that any person acting on behalf of the customer is so authorised, and should verify the identity of that person.

37. The identity of customers, beneficial owners, as well as persons acting on their behalf, should be verified by using reliable, independent source documents, data or information. When relying on documents, a bank should be aware that the best documents for the verification of identity are those most difficult to obtain illicitly or to counterfeit. When relying on other sources than documents, the bank must ensure that the methods (which may include checking references with other financial institutions and obtaining financial statements) and sources of information are appropriate, and in accordance with the bank's policies and procedures and risk profile of the customer. A bank may require customers to complete a written declaration of the identity and details of the beneficial owner, although the bank should not rely solely on such declarations. As for all elements of the CDD process, a bank should also consider the nature and level of risk presented by a customer when determining the extent of the applicable due diligence measures.[26] In no case should a bank disregard its customer identification and verification procedures just because the customer is unable to be present for an interview (non-face-to-face customer); the bank should also take into account risk factors such as why the customer has chosen to open an account far away from its seat/office, in particular in a foreign jurisdiction. It would also be important to take into account the relevant risks associated with customers from jurisdictions that are known to have AML/CFT strategic deficiencies and apply enhanced due diligence when this is called for by the FATF, other international bodies or national authorities.

38. While the customer identification and verification process is applicable at the outset of the relationship or before an occasional banking transaction is carried out, a bank should use this information to build an understanding of the customer's profile and behaviour. The purpose of the relationship or the occasional banking transaction, the level of assets or the size of transactions of the customer, and the regularity or duration of the relationship are examples of information typically collected. Therefore, a bank

22 "Person" in this context refers to natural and legal persons or legal arrangements.

23 The term "beneficial owner" is used in this guidance paper consistently with the definition and clarifications provided by the FATF standards. As a reminder, the FATF defines a "beneficial owner" as the natural person(s) who ultimately owns or controls a customer and/or 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.

24 See Interpretive note to Recommendation 1 of the FATF. This requirement applies unless the country has determined through a risk assessment that particular types of activities (and customers associated with the activities) may, on a limited basis, be exempted because there is a proven low risk of ML or FT in line with the interpretive note to Recommendation 1.

25 See BCP 29, essential criterion 5(b) in *Core principles for effective banking supervision*, September 2012.

26 See World Bank, *Politically Exposed Persons, Preventive Measures for the Banking Sector,* 2010.

should also have policies and procedures in place to conduct due diligence on its customers sufficient to develop customer risk profiles either for particular customers or categories of customers. The information collected for this purpose should be determined by the level of risk associated with the customer's business model and activities as well as the financial products or services requested by the customer. These risk profiles will facilitate the identification of any account activity that deviates from activity or behaviour that would be considered "normal" for the particular customer or customer category and could be considered as unusual, or even suspicious. Customer risk profiles will assist the bank in further determining if the customer or customer category is higher-risk and requires the application of enhanced CDD measures and controls. The profiles should also reflect the bank's understanding of the intended purpose and nature of the business relationship/occasional banking transaction, expected level of activity, type of transactions, and, where necessary, sources of customer funds, income or wealth as well as other similar considerations. Any significant information collected on customer activity or behaviour should be used in updating the bank's risk assessment of the customer.

39. A bank should obtain customer identification papers as well as any information and documentation obtained as a result of CDD conducted on the customer. This could include copies of or records of official documents (eg passports, identity cards, driving licences), account files (eg financial transaction records) and business correspondence, including the results of any analysis undertaken such as the risk assessment and inquiries to establish the background and purpose of the relationships and activities.

40. A bank should also obtain all the information necessary to establish to its full satisfaction the identity of their customer and the identity of any person acting on behalf of the customer and of beneficial owners. While a bank is required to both identify its customers and verify their identities, the nature and extent of the information required for verification will depend on risk assessment, including the type of applicant (personal, corporate etc), and the expected size and use of the account. The specific requirements involved in ascertaining the identity of natural persons are usually prescribed in national legislation. Higher-risk customers will require the application of enhanced due diligence to verify customer identity. If the relationship is complex, or if the size of the account is significant, additional identification measures may be advisable, and these should be determined based on the level of overall risk.

41. When a bank is unable to complete CDD measures, it should not open the account, commence business relations or perform the transaction. However, there may be circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business. In such circumstances, the bank should adopt adequate risk management procedures with respect to the conditions and restrictions under which a customer may utilise the banking relationship prior to verification. In situations where an account has been opened but problems of verification arise during the course of the establishment of the banking relationship that cannot be resolved, the bank should close or otherwise block access to the account. In any event, the bank should consider filing a STR in cases where there are problems with completion of the CDD measures.[27] Additionally, where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/FT, banks should not voluntarily agree to open accounts with such customers. In such situations, banks should file an STR with the relevant authorities accordingly and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

42. A bank should have in place procedures and material capacity enabling front office, customer-facing activities to identify any designated entities or individuals (eg terrorists, terrorist organisations) in accordance with their national legislation and the relevant United Nations Security Council Resolutions (UNSCRs).

[27] Subject to any national legislation concerning handling of suspicious transactions.

43. While the transfer of funds from an account in the customer's name in another bank subject to the same CDD standard as the initial deposit may provide some comfort, a bank should nevertheless conduct its own due diligence and consider the possibility that the previous account manager may have asked for the account to be closed because of a concern about illicit activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant has been refused banking facilities by another bank due to concerns over illicit activities of the customer, it should consider classifying that applicant as higher-risk and apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

44. A bank should not open an account or conduct ongoing business with a customer who insists on anonymity or who gives an obviously fictitious name. Nor should confidential numbered[28] accounts function as anonymous accounts but they should be subject to exactly the same CDD procedures as all other customers' accounts, even if the procedures are carried out by selected staff. While a numbered account can offer additional confidentiality for the account-holder, the identity of the latter must be verified by the bank and known to a sufficient number of staff to facilitate the conduct of effective due diligence, especially if other risk factors indicate that the customer is higher-risk. A bank should ensure that its internal control, compliance, audit and other oversight functions, in particular the chief AML/CFT officer, and the bank's supervisors, have full access to this information as needed.

4. Ongoing monitoring

45. Ongoing monitoring is an essential aspect of effective and sound ML/FT risk management. A bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity. Without such knowledge, the bank is likely to fail in its obligations to identify and report suspicious transactions to the appropriate authorities. Ongoing monitoring should be conducted in relation to all business relationships and transactions, but the extent of the monitoring should be based on risk as identified in the bank risk assessment and its CDD efforts. Enhanced monitoring should be adopted for higher-risk customers or transactions. A bank should not only monitor its customers and their transactions, but should also carry out cross-sectional product/service monitoring in order to identify and mitigate emerging risk patterns.

46. All banks should have systems in place to detect unusual or suspicious transactions or patterns of activity. In establishing scenarios for identifying such activity, a bank should consider the customer's risk profile developed as a result of the bank's risk assessment, information collected during its CDD efforts, and other information obtained from law enforcement and other authorities in its jurisdiction. For example, a bank may be aware of particular schemes or arrangements to launder proceeds of crime that may have been identified by authorities as occurring within its jurisdiction. As part of its risk assessment process, it will have assessed the risk that activity associated with such schemes or arrangements may be occurring within the bank through a category of customers, group of accounts, transaction pattern or product usage. Based on this knowledge, the bank should design and apply appropriate monitoring tools and controls to identify such activity. These could be through alert scenarios for computerised monitoring systems or setting limits for a particular class or category of activity, for instance.

47. Using CDD information, a bank should be able to identify transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer's normal and expected transactions.

[28] In a numbered account, the names of the customer and beneficial owner are known to the bank but are substituted by an account number or code name in subsequent documentation.

48. A bank should have established enhanced due diligence policies and procedures for customers who have been identified as higher-risk by the bank. In addition to established policies and procedures relating to approvals for account opening, a bank should also have specific policies regarding the extent and nature of required CDD, frequency of ongoing account monitoring and updating of CDD information and other records. The ability of the bank to effectively monitor and identify suspicious activity would require access to updated, comprehensive and accurate customer profiles and records.

49. A bank should ensure that they have appropriate integrated management information systems, commensurate with its size, organisational structure or complexity, based on materiality and risks, to provide both business units (eg relationship managers) and risk and compliance officers (including investigating staff) with timely information needed to identify, analyse and effectively monitor customer accounts. The systems used and the information available should support the monitoring of such customer relationships across lines of business and include all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer's behaviour or business profile and transactions made through a customer account that are unusual.

50. The bank should screen its customer database(s) whenever there are changes to sanction lists. The bank should also screen its customer database(s) periodically to detect foreign PEPs and other higher-risk accounts and subject them to enhanced due diligence.

5. Management of information

(a) Record-keeping

51. A bank should ensure that all information obtained in the context of CDD is recorded. This includes both (i) recording the documents the bank is provided with when verifying the identity of the customer or the beneficial owner, and (ii) transcription into the bank's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

52. A bank should also develop and implement clear rules on the records that must be kept to document due diligence conducted on customers and individual transactions. These rules should take into account, if possible, any prescribed privacy measures. They should include a definition of the types of information and documentation that should be included in the records as well as the retention period for such records, which should be at least five years from the termination of the banking relationship or the occasional transaction.[29] Even if accounts are closed, in the event of ongoing investigation/ litigation, all records should be retained until the closure of the case. Maintaining complete and updated records is essential for a bank to adequately monitor its relationship with its customer, to understand the customer's ongoing business and activities, and, if necessary, to provide an audit trail in the event of disputes, legal action, or inquiries or investigations that could lead to regulatory actions or criminal prosecution.

53. Adequate records documenting the evaluation process related to ongoing monitoring and review and any conclusions drawn should also be maintained and will help to demonstrate the bank's compliance with CDD requirements and ability to manage ML and FT risk.

(b) Updating of information

54. Only if banks ensure that records remain accurate, up-to-date and relevant by undertaking regular reviews of existing records and updating the CDD information can other competent authorities, law enforcement agencies or financial intelligence units make effective use of that information in order to fulfil their own responsibilities in the context of AML/CFT. In addition, keeping up-to-date information will enhance the bank's ability to effectively monitor the account for unusual or suspicious activities.

[29] See BCP 29, essential criterion 5(f) in *Core principles for effective banking supervision*, September 2012.

(c) Supplying information to the supervisors

55. A bank should be able to demonstrate to its supervisors, on request, the adequacy of its assessment, management and mitigation of ML/FT risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT.

6. Reporting of suspicious transactions and asset freezing

(a) Reporting of suspicious transactions

56. Ongoing monitoring and review of accounts and transactions will enable banks to identify suspicious activity, eliminate false positives and report promptly genuine suspicious transactions. The process for identifying, investigating and reporting suspicious transactions to the FIU should be clearly specified in the bank's policies and procedures and communicated to all personnel through regular training. These policies and procedures should contain a clear description for employees of their obligations and instructions for the analysis, investigation and reporting of such activity within the bank as well as guidance on how to complete such reports.

57. There should also be established procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement agency or FIU and/or supervisory authorities, if relevant. These procedures should also reflect the principle of confidentiality, ensure that investigation is conducted swiftly and that reports contain relevant information and are produced and submitted in a timely manner. The chief AML/CFT officer should ensure prompt disclosures where funds or other property that is suspected to be the proceeds of crime remain in an account.

58. Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity a bank should ensure that appropriate action is taken to adequately mitigate the risk of the bank being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FIU.

(b) Asset freezing

59. Financing of terrorism has similarities compared to money laundering, but it also has specificities that banks should take into due consideration: funds that are used to finance terrorist activities may be derived either from criminal activity or from legal sources, and the nature of the funding sources may vary according to the type of terrorist organisation. In addition, it should be noted that transactions associated with the financing of terrorists may be conducted in very small amounts.

60. A bank should be able to identify and to enforce funds freezing decisions made by the competent authority and it should otherwise not deal with any designated entities or individuals (eg terrorists, terrorist organisations) consistent with relevant national legislation and UNSCRs.

61. CDD should help a bank to detect and identify potential FT transactions, providing important elements for a better knowledge of its customers and the transactions they conduct. In developing customer acceptance policies and procedures, a bank should give proper relevance to the specific risks of entering into or pursuing business with individuals or entities linked to terrorist groups. Before establishing a business relationship or carrying out an occasional transaction with new customers, a bank should screen customers against lists of known or suspected terrorists issued by competent (national and international) authorities. Likewise, ongoing monitoring should verify that existing customers are not entered into these same lists.

62. All banks should have systems in place to detect prohibited transactions (eg transactions with entities designated by the relevant UNSCRs or national sanctions). Terrorist screening is not a risk-sensitive due diligence measure and should be carried out irrespective of the risk profile attributed to the customer. For the purpose of terrorist screening, a bank may adopt automatic screening systems, but it should ensure that such systems are fit for the purpose. A bank should freeze without delay and without prior notice the funds or other assets of designated persons and entities, following applicable laws and regulations.

III. AML/CFT in a group-wide and cross-border context

63. Sound ML/FT risk management where a bank operates in other jurisdictions entails consideration of host country legal requirements. Given the risks, each group should develop group-wide AML/CFT policies and procedures consistently applied and supervised across the group. In turn, policies and procedures at the branch or subsidiary levels, even though reflecting local business considerations and the requirements of the host jurisdiction, must still be consistent with and supportive of the group's broader policies and procedures.[30] In cases where the host jurisdiction requirements are stricter than the group's, group policy should allow the relevant branch or subsidiary to adopt and implement the host jurisdiction local requirements.

1. Global process for managing customer risks

64. Consolidated risk management means establishing and administering a process to coordinate and apply policies and procedures on a group-wide basis, thereby implementing a consistent and comprehensive baseline for managing the bank's risks across its international operations. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate group-wide risks. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements. In this regard, a bank should have robust information-sharing among the head office and all of its branches and subsidiaries. Where the minimum regulatory or legal requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two.

65. Furthermore, according to FATF Standards,[31] if the host country does not permit the proper implementation of those standards, the chief AML/CFT officer should inform the home supervisors. Additional measures should be considered, including, as appropriate, the financial group closing its operations in the host country.

66. The Committee recognises that implementing group-wide AML/CFT procedures is more challenging than many other risk management processes because some jurisdictions continue to restrict the ability of banks to transmit customer names and balances across national borders. For effective group-wide monitoring and for ML/FT risk management purposes, it is essential that banks be authorised to share information about their customers, subject to adequate legal protection, with their head offices or parent bank. This applies in the case of both branches and subsidiaries.

[30] The term "group" is used in this paper to refer to an organisation's one or more banks, and the branches and subsidiaries of those banks. The term "head office" is used in this paper to refer also to the parent bank or to the unit in which AML/CFT risk management is performed on a business line basis.

[31] See Interpretative Note to recommendation 18 (Internal controls and foreign branches and subsidiaries) in the FATF Standards.

2. Risk assessment and management

67. The bank should have a thorough understanding of all the risks associated with its customers across the group, either individually or as a category, and should document and update these on a regular basis, commensurate with the level and nature of risk in the group. In assessing customer risk, a bank should identify all relevant risk factors such as geographical location and patterns of transaction activity (declared or self-stated) and usage of bank products and services and establish criteria for identifying higher-risk customers. These criteria should be applied across the bank, its branches and its subsidiaries and through outsourced activities (see Annex 1). Customers that pose a higher risk of ML/FT to the bank should be identified across the group using these criteria. Customer risk assessments should be applied on a group-wide basis or at least be consistent with the group-wide risk assessment. Taking into account differences in risks associated with customer categories, group policy should recognise that customers in the same category may pose different risks in different jurisdictions. The information collected in the assessment process should then be used to determine the level and nature of overall group risk and support the design of appropriate group controls to mitigate these risks. The mitigating factors can comprise additional information from the customer, tighter monitoring, more frequent updating of personal data and visits by bank staff to the customer location.

68. Banks' compliance and internal audit staff, in particular the chief AML/CFT officer, or external auditors, should evaluate compliance with all aspects of their group's policies and procedures, including the effectiveness of centralised CDD policies and the requirements for sharing information with other group members and responding to queries from head office. Internationally active banking groups should ensure that they have a strong internal audit and a global compliance function since these are the primary mechanisms for monitoring the overall application of the bank's global CDD and the effectiveness of its policies and procedures for sharing information within the group. This should include the responsibility of a chief AML/CFT officer for group-wide compliance with all relevant AML/CFT policies, procedures and controls nationally and abroad (see paragraphs 75 and 76).

3. Consolidated AML/CFT policies and procedures

69. A bank should ensure it understands the extent to which AML/CFT legislation allows it to rely on the procedures undertaken by other banks (for example within the same group) when business is being referred. A bank should not rely on introducers that are subject to standards that are less strict than those governing the bank's own AML/CFT procedures. This will entail banks monitoring and evaluating the AML/CFT standards in place in the jurisdiction of the referring bank. A bank may rely on an introducer that is part of the same financial group and could consider placing a higher level of reliance on the information provided by this introducer, provided this introducer is subject to the same standards as the bank, and the application of these requirements is supervised at the group level. A bank taking this approach should ensure, however, that it obtains customer information from the referring bank (as further detailed in Annex 1), as this information may be required to be reported to FIUs in the event that a transaction involving the referred customer is determined to be suspicious.

70. Relevant information should be accessible by the banking group's head office for the purpose of enforcing group AML/CFT policies and procedures. Each office of the banking group should be in a position to comply with minimum AML/CFT and accessibility policies and procedures applied by the head office and defined consistently with the Committee guidelines.

71. Customer acceptance, CDD and record-keeping policies and procedures should be implemented through the consistent application of policies and procedures throughout the organisation, with adjustments as necessary to address variations in risk according to specific business lines or geographical areas of operation. Moreover, it is recognised that different approaches to information collection and retention may be necessary across jurisdictions to conform to local regulatory requirements or relative risk factors. However, these approaches should be consistent with the group-wide standards discussed above.

72. Regardless of its location, each office should establish and maintain effective monitoring policies and procedures that are appropriate to the risks present in the jurisdiction and in the bank. This local monitoring should be complemented by a robust process of information-sharing with the head office, and if appropriate with other branches and subsidiaries regarding accounts and activity that may represent heightened risk.

73. To effectively manage the ML and FT risks arising from such accounts, a bank should integrate this information based not only on the customer but also on its knowledge of both the beneficial owners of the customer and the funds involved. A bank should monitor significant customer relationships, balances and activity on a consolidated basis, regardless of whether the accounts are held on-balance sheet, off-balance sheet, as assets under management or on a fiduciary basis, and regardless of where they are held. The FATF standards have now also set out more details relating to banks' head office oversight of group compliance, audit and/or AML/CFT functions.[32] Moreover, if these guidelines have been conceived primarily for banks, they might be of interest for conglomerates (including banks).

74. Many large banks with the capability to do so centralise certain processing systems and databases for more effective management or efficiency purposes. In implementing this approach, a bank should adequately document and integrate the local and centralised transaction/account monitoring functions to ensure that it has the opportunity to monitor for patterns of potential suspicious activity across the group and not just at either the local or centralised levels.

75. A bank performing business nationally and abroad should appoint a chief AML/CFT officer for the whole group (group AML/CFT officer). The group AML/CFT officer has responsibility, as a part of the global risk management, for creating, coordinating and group-wide assessment of the implementation of a single AML/CFT strategy (including mandatory policies and procedures and the authorisation to give orders for all branches, subsidiaries and subordinated entities nationally and abroad).

76. The function of the group AML/CFT officer includes ongoing monitoring of the fulfilment of all AML/CFT requirements on a group-wide basis, nationally and abroad. Therefore, the group AML/CFT officer should satisfy him/herself (including through on-site visits on a regular basis) that there is group-wide compliance with the AML/CFT requirements. If needed, he/she should be empowered to give orders or take the necessary measures for the whole group.

4. Group-wide information-sharing

77. Banks should oversee the coordination of information-sharing. Subsidiaries and branches should be required to proactively provide the head office with information concerning higher-risk customers and activities relevant to the global AML/CFT standards, and respond to requests for account information from the head office or parent bank in a timely manner. The bank's group-wide standards should include a description of the process to be followed in all locations for identifying, monitoring and investigating potential unusual circumstances and reporting suspicious activity.

78. The bank's group-wide policies and procedures should take into account issues and obligations related to local data protection and privacy laws and regulations. They should also take into account the different types of information that may be shared within a group and the requirements for storage, retrieval, sharing/distribution and disposal of this information.

79. The group's overall ML/FT risk management function should evaluate the potential risks posed by activity reported by its branches and subsidiaries and, where appropriate, assess the group-wide risks presented by a given customer or category of customers. It should have policies and procedures to ascertain if other branches or subsidiaries hold accounts for the same customer (including any related or affiliated parties). The bank should also have policies and procedures governing global account

[32] See in particular Recommendation 18 in the FATF Standards.

relationships that are deemed higher-risk or have been associated with potentially suspicious activity, including escalation procedures and guidance on restricting account activities, including the closing of accounts as appropriate.

80. In addition, a bank and its branches and subsidiaries should, in accordance with their respective domestic laws, be responsive to requests from law enforcement agencies, supervisory authorities or FIUs for information about customers that is needed in their efforts to combat ML and FT. A bank's head office should be able to require all branches and subsidiaries to search their files against specified lists or requests for individuals or organisations suspected of aiding and abetting ML and FT, and report matches.

81. A bank should be able to inform its supervisors, if so requested, about its global process for managing customer risks, its risk assessment and management of ML/FT risks, its consolidated AML/CFT policies and procedures, and its group-wide information-sharing arrangements.

5. Mixed financial groups

82. Many banking groups engage in securities and insurance businesses. The application of ML/FT risk management controls in mixed financial groups poses additional issues that may not be present for deposit-taking and lending operations. Mixed groups should have the ability to monitor and share information on the identity of customers and their transaction and account activities across the entire group, and be alert to customers that use their services in different sectors, as described in paragraph 79 above.

83. Differences in the nature of activities and patterns of relationships between banks and customers in each sector may require or justify variations in the AML/CFT requirements imposed on each sector. The group should be alert to these differences when cross-selling products and services to customers from different business arms, and the appropriate AML/CFT requirements for the relevant sectors should be applied.

IV. The role of supervisors

84. Banking supervisors are expected to comply with FATF Recommendation 26, which states in part: "For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and financing of terrorism, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes." The Committee expects supervisors to apply the *Core principles for effective banking supervision* to banks' ML/FT risk management in a manner consistent with and supportive of the supervisors' overall supervision of banks. Supervisors should be able to apply a range of effective, proportionate and dissuasive sanctions in cases when banks fail to comply with their AML/CFT requirements.

85. Banking supervisors are expected to set out supervisory expectations governing banks' AML/CFT policies and procedures. The essential elements as set out in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice. National supervisors are encouraged to provide guidance to assist banks in designing their own customer identification policies and procedures. The Committee has therefore developed two specific topic guides in Annexes 1 and 2, which could be used by supervisors for this purpose.

86. Supervisors should adopt a risk-based approach to supervising banks' ML/FT risk management.[33] Such an approach requires that supervisors (i) develop a thorough understanding of the risks present in the jurisdiction and their potential impact on the supervised entities; [34] (ii) evaluate the adequacy of the bank's risk assessment based on the jurisdiction's national risk assessment(s);[35] (iii) assess the risks present in the target supervised entity to understand the nature and extent of the risks in the entity's customer base, products and services and the geographical locations in which the bank and its customers do business; (iv) evaluate the adequacy and effectiveness in implementation of the controls (including CDD measures) designed by the bank in meeting its AML/CFT obligations and risk mitigation; and (v) utilise this information to allocate the resources, scope the review, identify the necessary supervisory expertise and experience needed to conduct an effective review and allocate these resources relative to the identified risks.

87. Higher-risk lines of business or customer categories may require specialised expertise and additional procedures to ensure an effective review. The bank's risk profile should also be used in determining the frequency and timing of the supervisory cycle. Again, banks dealing with higher risk profiles may require more frequent review than others. Supervisors should also verify whether banks have adequately used their discretion with regard to applying AML/CFT measures on a risk-based approach. They should also evaluate the internal controls in place and how banks determine whether they are in compliance with supervisory and regulatory guidance, and prescribed obligations. The supervisory process should include not only a review of policies and procedures but also, when appropriate, a review of customer documentation and the sampling of accounts and transactions, internal reports and STRs. Supervisors should always have the right to access all documentation related to the transactions conducted or accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

88. Supervisors have a duty to ensure their banks maintain sound ML/FT risk management not only to protect their own safety and soundness but also to protect the integrity of the financial system.[36] Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors (or other relevant national authorities) should be able to apply appropriate countermeasures and ensure that banks are aware of and apply enhanced CDD measures to business relationships and to transactions when called for by the FATF or that involve jurisdictions where their AML/CFT standards are considered inadequate by the country. In this aspect, the FATF and some national authorities have listed a number of countries and jurisdictions

[33] Supervisors should also take into account the risk-based approach to supervision described in Interpretive Note 26 in the FATF Standards.

[34] For this, it is expected that supervisors would build on countries' assessment such as described in the interpretative note to recommendation 1 in the FATF standards.

[35] Including, where appropriate, any supranational risk assessment.

[36] Many supervisors also have a duty to report any suspicious, unusual or illegal transactions that they detect, for example, during on-site examinations.

that are considered to have strategic AML/CFT deficiencies or that do not comply with international AML/CFT standards,[37] and such findings should be a component of a bank's ML/FT risk management.

89. Supervisors should also consider a bank's overall monitoring and oversight of compliance at the branch and subsidiary level as well as the ability of group policy to accommodate local regulatory requirements and ensure that where there is a difference between the group and local requirements, the stricter of the two is applied. Supervisors should also ensure that in cases where the group branch or subsidiary cannot apply the stricter of the two standards, the reasons for this and the differences between the two should be documented and appropriate mitigating measures implemented to address risks identified as a result of those differences.

90. In a cross-border context, home country supervisors[38] should face no impediments in verifying a bank's compliance with group-wide AML/CFT policies and procedures during on-site inspections. This may well require a review of customer files and a sampling of accounts or transactions in the host jurisdiction. Home country supervisors should have access to information on sampled individual customer accounts and transactions and on the specific domestic and international risks associated with such customers to the extent necessary to enable a proper evaluation of the application of CDD standards and an assessment of risk management practices. This use of information for a legitimate supervisory need, safeguarded by the confidentiality provisions applicable to supervisors, should not be impeded by local bank secrecy or data protection laws. Although the host country supervisors and/or other authorities retain responsibility for the enforcement of compliance with local AML/CFT requirements (which would include an evaluation of the appropriateness of the procedures), host country supervisors should ensure they extend full cooperation and assistance to home country supervisors who may need to assess how the bank oversees compliance with group-wide AML/CFT policies and processes.

91. The role of group audit (external or internal) is particularly important in assessing the effectiveness of AML/CFT policies and procedures. Home country supervisors should ensure that there is an appropriate policy, based on the risks, and adequate resources allocated regarding the scope and frequency of audit of the group's AML/CFT. They should also ensure that auditors have full access to all relevant reports during the audit process.

92. Supervisors should ensure that information about banks' customers and transactions is subject to the same confidentiality measures as are applicable to the broad array of information shared between supervisors on banks' activities.

93. It is essential that all jurisdictions that host foreign banks provide an appropriate legal framework to facilitate the passage of information required for customer risk management purposes to the head office or parent bank and home country supervisors. Similarly, there should be no impediments to on-site visits to host jurisdiction subsidiaries and branches by home jurisdiction head office auditors, risk managers, compliance officers (including the chief AML/CFT officer and/or AML/CFT group officer), or home country supervisors, nor any restrictions in their ability to access all the host jurisdiction bank's records, including customers' names and balances. This access should be the same for both branches and subsidiaries. If impediments to information-sharing prove to be insurmountable, and there are no

[37] For instance, jurisdictions may be publicly identified by :

- the FATF's *Public Statement*, which identifies:
  - (i) jurisdictions that have strategic AML/CFT deficiencies and to which countermeasures apply;
  - (ii) jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.
- The FATF public document, *Improving Global AML/CFT Compliance: On-going Process*, which identifies jurisdictions with strategic AML/CFT deficiencies that have provided a high-level political commitment to address the deficiencies through implementation of an action plan developed with the FATF.

[38] In those countries where the examination process is undertaken by external auditors, this exemption should also apply to the competent auditors.

satisfactory alternative arrangements, the home supervisors should make it clear to the host supervisor that the bank may be subject to additional supervisory actions, such as enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host jurisdiction.

94. Where a bank's head office staff are granted access to information on local customers, there should be no restrictions on them reporting such information back to head office. Such information should be subject to adequate safeguards on confidentiality and use and may be subject to applicable privacy and privilege laws in the home country.

95. The Committee believes that there is no justifiable reason why local legislation should impede the transfer of customer information from a host bank branch or subsidiary to its head office or parent bank in the home jurisdiction for risk management purposes, including ML and FT risks. If the law in the host jurisdiction restricts disclosure of such information to "third parties", it is essential that the head office or parent bank and the home jurisdiction bank supervisors are clearly excluded from definitions of a third party. Jurisdictions that have legislation that impedes, or can be interpreted as impeding, such information-sharing for ML/FT risk management purposes, are urged to remove any such restrictions and to provide specific gateways appropriate for this purpose.

96. Prudential and AML/CFT supervisors should establish an effective cooperation mechanism regardless of the institutional setting, as set out in Annex 5, to ensure that ML/FT risks are adequately supervised in the domestic and cross-jurisdictional context for the benefit of the two functions.

Annex 1

Using another bank, financial institution or third party to perform customer due diligence

I. Introduction

1. In some countries, banks are permitted to use other banks, financial institutions or other entities to perform customer due diligence (CDD). These arrangements can take various forms but in essence usually fall into one of the following two situations:

Reliance on third parties

2. Banks in some countries are allowed to rely on CDD performed by other financial institutions or designated non-financial businesses and professions who are themselves supervised or monitored for AML/CFT purposes.[39] In these situations, the third party will usually have an existing business relationship with the customer, and the banks may be exempt from applying their own CDD measures at the beginning of the relationship. The FATF standards[40] permit reliance for these aspects:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

FATF standards further require that a financial institution relying upon a third party should immediately obtain the necessary information concerning these three CDD measures.

3. Some countries restrict the ability to rely in various ways; for example, limiting reliance to financial institutions, allowing reliance only for third parties' existing relationships (and prohibiting chains of reliance) or not allowing reliance on foreign entities.

Outsourcing/agency

4. Banks may also use third parties to perform various elements of their CDD obligations on a contractual basis, often in an outsourcing/agent relationship (ie the outsourced entity applies the CDD measures on behalf of the delegating bank). Typically, there are fewer restrictions on who can act as the agent of a bank, but this is often offset by prescribed arrangements and record-keeping.

5. For both reliance and outsourcing, banks may choose to limit the size, scope or nature of transaction types when utilising third parties. In all cases, supervisors should have timely access to

[39] See Recommendation 17 in the FATF Standards and its interpretative note.

[40] See Recommendation 17 and Recommendation 10 on CDD in the FATF Standards.

customer information upon request. Although these two categories seem similar or related, there are significant differences between them and banks should ensure they understand those differences and reflect these in their policies and procedures.

II. Reliance on third parties

6. Banks should have clear policies and procedures on whether and when it is acceptable and prudent to rely on another bank or financial institution. Such reliance in no way relieves the bank of its ultimate responsibility for having adequate CDD policies and procedures and other AML/CFT requirements on customers, such as understanding expected activity, whether customers are high-risk, and whether transactions are suspicious.

7. In depending on another bank or financial institution to conduct certain aspects of CDD, banks should assess the reasonableness of such reliance. In addition to ensuring there is a legal ability to rely, relevant criteria for assessing reliance include:

(a) The bank, financial institution or other entity (as permitted by national law) on which reliance is placed should be as comprehensively regulated and supervised as the bank, have comparable customer identification requirements at account opening and have an existing relationship with the customer opening an account at the bank. Alternatively, national law may require the use of compensating measures or controls, in cases where these standards are not met.

(b) The bank and the other entity should have an arrangement or understanding in writing acknowledging the bank's reliance on the other financial institution's CDD processes.

(c) The bank's procedures and policies should document the reliance and should establish adequate controls and review procedures for such a relationship.

(d) A third party may be required to certify to the bank that it has implemented its AML programme, and that it performs CDD substantially equivalent to or consistent with the bank`s obligations.

(e) The bank should give due consideration to adverse public information about the third party, such as its subjection to an enforcement action for AML deficiencies or violations.

(f) The bank should identify and mitigate any additional risk posed by reliance on multiple parties (a chain of reliance) rather than a direct relationship with one entity.

(g) The bank's risk assessment should identify reliance on third parties as a potential risk factor.

(h) The bank should periodically review the other entity to ensure that it continues to conduct CDD in a manner as comprehensive as the bank. For that purpose, the bank should obtain all the CDD information and documents from the bank, financial institution, or entity that it relies upon and assess due diligence conducted, including screening against local databases to ensure compliance with local regulatory requirements.

(i) Banks should consider terminating reliance on entities that do not apply adequate CDD on their customers or otherwise fail to meet requirements and expectations.

8. Banks with subsidiaries or branches outside the home jurisdiction frequently use the financial group to introduce their customers to other parts of the financial group. In countries that permit this cross-border reliance on affiliates, financial institutions that rely on other parts of the group for customer identification should ensure that the above assessment criteria are in place. The FATF standards[41] allow

[41] See Recommendation 17 in the FATF Standards.

countries to exempt country risk from this assessment if the financial institution is subject to group-wide AML/CFT standards and supervised on a group level by its financial supervisor.

III. Outsourcing/agency

9. Banks may choose to apply identification and other CDD processes directly or can appoint one or more third parties to take these measures on their behalf, sometimes in an agent relationship. While AML/CFT compliance functions may be performed by third parties, the responsibility for complying with CDD and AML/CFT requirements remains with the bank. The extent of the use of third parties usually depends on the business model of the bank; normally, banks that operate by telephone or over the internet or that have few "bricks & mortar" branches tend to use third parties to a greater extent. Banks may use third parties to expand their customer base or improve customer support and overall access to their services.

10. Banks that choose to use third parties should ensure that a written agreement is in place that sets out the AML/CFT obligations of the bank and how these will be executed by the third party. In some countries, the relationship between banks and their third parties is regulated.

11. As noted above, it is important for banks to understand the difference between using a third party as its agent and relying on another bank's customer identification and CDD processes. An agent is usually, under the law of agent and principal, a legal extension of the bank. When a bank's customer or potential customer deals with an agent of a bank, it is legally dealing with the bank itself. The third party will therefore be obligated to apply the bank's policies and requirements with respect to identification and verification and CDD.

12. In practice, banks' third parties need to have the necessary technical expertise, knowledge and training to apply customer identification and CDD measures of the bank. In some cases, where third parties' business models are based on acting for several banks, they usually develop significant in-house expertise of their own. However, third parties are not always themselves subject to AML/CFT obligations, although many often are. Whether or not this is the case, however, the third party is always in the position of applying its principal's identification and CDD requirements (which in turn must conform to legal requirements).

13. Examples of third parties routinely used by banks to apply their customer identification obligations include retail deposit brokers, mortgage brokers and solicitors. ML/FT risk mitigation can be compromised when banks do not ensure that applicable customer identification requirements and CDD are applied by their third parties.

14. As noted, there should be a written agreement or arrangement documenting the third party's responsibilities, which should include the following:

(a) requiring the application of the bank's customer identification and CDD requirements (including enquiring on source of funds and wealth, as appropriate);

(b) ensuring that, where the customer is present in person at the time customer identification and/or CDD measures are conducted, the third party applies customer identification procedures that include viewing original identification documents where this is required by regulations or the bank;

(c) ensuring that, where the customer is not present at the time customer identification is ascertained, the third party applies any applicable prescribed or bank-stipulated non-face-to-face identification requirements; and

(d) ensuring that the third party maintains the confidentiality of customer information.

15. Banks should also:

(a) ensure that if the third party is responsible for determining and/or identifying the beneficial owner or a PEP determination, these responsibilities are documented;

(b) ensure that the third party provides the bank with customer identification information in the required time frames; and

(c) periodically review or audit, in a systemic manner, the quality of customer information gathered and documented by the third party to ensure that it continues to meet the bank's requirements;

(d) clearly identify instances that the bank would consider failures on the part of the third party to perform its duties as contracted and establish a process for implementing appropriate actions, such as terminating the relationship in response to identified failures.

16. The bank should obtain all relevant information from the third party in a timely manner and ensure the information is complete and kept up to date in the bank's customer record.

17. Contracts with third parties should be reviewed and updated as necessary to ensure that they continue to address the third parties' role accurately and reflect any updates to duties.

Annex 2

Correspondent banking

I. General considerations on cross-border correspondent banking

1. According to the FATF glossary, "correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank')". For the purpose of its guidance on correspondent banking (hereafter "the FATF guidance"),[42] the FATF does not include one-off transactions or the mere exchange of messaging capabilities[43] but rather states that correspondent banking is characterised by its ongoing, repetitive nature. Like the FATF guidance, this Annex focuses on higher-risk correspondent banking relationships, in particular cross border correspondent banking involving the execution of third-party payments. Indeed, in line with FATF Recommendation 13, cross-border correspondent relationships (as opposed to domestic relationships) are the ones that should prompt additional customer due diligence measures.

2. Used by banks throughout the world, correspondent banking services enable respondent banks to conduct business and provide services[44] that they cannot offer otherwise (owing to the lack of an international presence and cross-border payment systems). As noted by the Financial Stability Board, the ability to make and receive international payments via correspondent banking is vital for businesses and individuals, and for the G20's goal of strong, sustainable, balanced growth.[45]

3. Correspondent banks that execute and/or process transactions for customers of respondent banks generally do not have direct business relationships with these customers, which may be individuals, corporations or financial services firms, established in jurisdictions other than that of the correspondent bank. Thus the customers of the correspondent bank are the respondent banks. Correspondent banks are therefore required to conduct appropriate due diligence on the respondent banks and are not generally required to do so on the respondent banks' customers.[46]

4. Because of the structure of this activity and the limited information available regarding the nature or purpose of the underlying transactions, correspondent banks may be exposed to money laundering and financing of terrorism (ML/FT) risks.

[42] FATF, *Guidance on correspondent banking services*, October 2016, www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html.

[43] Such as SWIFT Relationship Management Application (RMA) keys.

[44] Such as "cash management (eg interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services", FATF Glossary in the FATF recommendations.

[45] See FSB, *Progress report to G20 on the FSB action plan to assess and address the decline in correspondent banking,* August 2016, www.fsb.org/2016/08/progress-report-to-g20-on-the-fsb-action-plan-to-assess-and-address-the-decline-in-correspondent-banking/.

[46] See FATF, *Guidance on correspondent banking services*, October 2016, paragraph 3: "The term KYCC has created a lot of confusion. To clarify, the FATF Recommendations do not require financial institutions to conduct customer due diligence on the customers of their customer (ie, each individual customer)."

5. Respondent banks are the ones responsible for conducting due diligence on their customers using correspondent banking services. The present guidance addresses both correspondent banks that provide the services and respondent banks that use the services.

6. If the respondent bank is an affiliate of the correspondent bank, the AML/CFT policies and procedures applicable at the consolidated group level apply to the respondent bank.[47]

II. Risk-based approach in the context of providing correspondent banking services

7. The FATF guidance clarifies that, while additional customer due diligence (CDD) measures are required for cross-border correspondent banking, not all such correspondent banking services carry the same level of ML/FT risks.[48] The FATF guidance focuses on higher-risk correspondent banking relationships, in particular, cross-border correspondent banking relationships involving the execution of third-party payments. This section provides factors that banks should consider when assessing the level of risk of a particular correspondent banking relationship.

A. Risk indicators and risk assessment

8. Banks that undertake correspondent banking activities should assess the ML/FT risks associated with the relationship.

9. Risk indicators that correspondent banks should consider in their risk assessment include:

(1) the inherent risk resulting from the nature of services provided, in particular:

- (a) the purpose of the services provided to the respondent bank (eg foreign exchange services for respondents' proprietary trading, securities trading on recognised exchanges or payments between a respondent's group within the same jurisdiction may constitute indicators of lower risk);
- (b) whether the banking services will be used, via nested (downstream) correspondent(s), by either the respondent bank's affiliates or other third parties, and the different risks these parties entail (see paragraph 12 below);
- (c) whether the banking services will be used, via payable-through-account(s) activity, by either the respondent bank's affiliates or other third parties, and the different risks these parties entail (see paragraph 29 below).

(2) the characteristics (and information on) of the respondent bank, in particular:

- (d) the respondent bank's major business activities including target markets and overall types of customers served in key business lines;[49]

[47] See section III in Basel Committee on Banking Supervision, *Sound management of risks related to money laundering and financing of terrorism*.

[48] See FATF, *Guidance on correspondent banking services*, October 2016, paragraph 13a.

[49] The correspondent bank should have a broad knowledge of the products and services offered and types of customers served by the respondent bank (see FATF guidance, paragraph 22).

(e) the respondent bank's management and ownership (including the beneficial owners) and whether they represent specific ML/FT risks (eg politically exposed persons (PEPs));

(f) the respondent bank's money laundering prevention and detection policies and procedures, including a description of the CDD measures applied by the respondent bank to its customers and the correspondent bank's ability to obtain information on a particular transaction as specified in paragraphs 32–3 of the FATF guidance;[50]

(g) whether any civil, administrative or criminal actions or sanctions, including public reprimands, have been applied by any court or supervisory authority to the respondent bank, when it occurred, the severity, and how the respondent bank addressed the identified shortcomings.

(3) the environment in which the respondent bank operates, in particular:

(h) the jurisdiction in which the respondent bank (and its parent company when the respondent bank is an affiliate) is located;

(i) the jurisdictions in which subsidiaries and branches of the group may be located, possibly using the group structure available in the Legal Entity Identifier (LEI) system,[51] as well as the jurisdictions in which third parties using the correspondent banking relationship may be located;

(j) the quality and effectiveness of banking regulation and supervision in the respondent's country (especially AML/CFT laws and regulations)[52] and the respondent's parent company country when the respondent is an affiliate.

10. Correspondent banks should take a holistic view of the above indicators and other available information, to first determine the inherent risk of each respondent bank relationship, and then to consider risk mitigation factors to determine the residual risk and whether it can manage this residual risk level (see FATF guidance, paragraph 16). In general, factors that could reduce ML/FT risks would include the effectiveness of the respondent bank's risk management policies and procedures as well as the specific measures put in place by the correspondent bank.

11. In some instances, inherently higher-risk relationships, products or services may be mitigated by strong risk management practices and other factual circumstances, resulting in adequately manageable residual risk. For example, a correspondent banking relationship with a foreign respondent bank located in a higher-risk foreign jurisdiction could pose an inherently higher risk that may be mitigated in part because of effective group-wide AML/CFT controls in place in both the correspondent and respondent banks. Correspondent banks can also manage their risk by adapting their product offering or limiting the volume of activity with a particular respondent.

[50] The ability to obtain this information may depend on legal or technical permissibility.

[51] Information on ultimate parents of legal entities started being collected in the LEI system in May 2017 and is available on the website of the Global LEI Foundation; information on branches will follow in 2017 (see LEI ROC, *Collecting data on direct and ultimate parents of legal entities in the Global LEI System – Phase 1*, 10 March 2016, and *Including data on international/foreign branches in the Global LEI System*, 11 July 2016). The LEI system may be used for that purpose provided that the group's ultimate accounting consolidating parent and all group entities in the accounting consolidation perimeter and eligible branches have an LEI, and that the ultimate parent relationship is reported for all subsidiaries. In addition, the relevant LEI should have an "issued" status (for active entities), which means that the associated reference data are kept current under the conditions required by the LEI System.

[52] See paragraph 25 of the FATF guidance.

B. Nested (downstream) correspondent banking

12. Nested, or downstream, correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

13. Downstream correspondent banking relationships are an integral and generally legitimate part of correspondent banking. Nesting may be a way for regional banks to help small local banks within the respondent's region obtain access to the international financial system or to facilitate transactions where no direct relationship exists between banks.

14. Providing access to third-party foreign financial institutions that are not the customer of the correspondent bank, and so not necessarily known, can obscure financial transparency and increase ML/FT risks. As a result, correspondent banks should require that respondent banks disclose whether accounts include nested relationships[53] as part of account opening and ongoing risk profile reviews. Respondent banks should disclose accurate information regarding the existence of nested relationships.

15. Correspondent banks should assess the ML/TF risk associated with customers which are respondent banks with nested relationships on an individual case by case basis, consistent with the risk-based approach. The level of risk may vary depending on the nature of nested foreign financial institutions served by respondent banks, including size and geographical location, products and services offered, markets and customers served, and the degree of transparency provided by the respondent bank (eg in formatting payment transactions).

16. In order to assess the ML/FT risks associated with a nested relationship, correspondent banks should understand the purpose of the nested relationship. To this end, they may consider the following factors, among others:

(a) the number and type of financial institutions a respondent bank serves;

(b) whether the nested banks are located in the same jurisdiction as the respondent (considering the knowledge a respondent bank might have of its own jurisdiction) or a different country;

(c) whether the jurisdiction of the nested bank and the areas the nested bank serves have adequate AML/CFT policies according to available public information (eg FATF information);

(d) the types of services the respondent offers to nested banks (proprietary only or customer services such as correspondent banking);

(e) the length of the relationship between the correspondent and respondent banks (eg a long-standing relationship which enables the correspondent bank to have a good understanding of the ML/FT risk associated with the relationship versus a new one);

(f) the adequacy of the due diligence programme of the respondent bank to evaluate the AML/CFT controls on its nested banks. The due diligence programme should be updated periodically and provided to the correspondent bank at its request.

17. Respondent banks should promptly respond to requests for information from correspondent banks (see FATF guidance, paragraphs 32–3) related to transactions through respondent banks, as appropriate.

C. Information-gathering

18. Before entering into a business relationship with a respondent bank, correspondent banks should gather sufficient information to understand the nature of the respondent's business and assess ML/FT risks

[53] This does not entail that a list of the nested relationships should be produced.

both at the outset and on an ongoing basis. There is no requirement or expectation for a correspondent bank to apply CDD measures to customers of the respondent bank or to duplicate the data on its customers obtained and stored by the respondent bank.

19. Information on a respondent bank's AML/CFT policies and procedures may be obtained from the respondent bank, for example via a questionnaire, or from publicly available information (such as financial information or any mandatory supervisory information relating to the respondent bank). An industry-wide questionnaire may be useful, provided it is used as a starting point for the risk assessment. The correspondent bank should verify the identity of the respondent bank using reliable, independent source documents, data or information (see Annex 4) and take measures to verify other CDD information on the respondent bank obtained on a risk-sensitive basis and identify any beneficial owners.

20. At account opening, banks may collect – and subsequently update – respondent banks' information by using third-party databases that contain relevant information on banks (often referred to as "KYC utilities"). KYC utilities may provide efficiency gains for both correspondent and respondent banks to gather and provide information, especially with regard to standardisation and interoperability (eg the ability of different systems to share data). From the correspondent bank perspective, using a KYC utility could in particular be useful for gathering information on the respondent bank, especially to assess the risk indicators listed in paragraph 9. If banks see benefits in using KYC utilities for obtaining information from the respondent bank, supervisors see in principle no objection to the use of utilities in correspondent banking risk assessment processes, provided the conditions and factors described in paragraphs 6bis and 6ter of Annex 4 are met and the final responsibility for CDD remains with the correspondent.

21. Banks should also consider gathering information from public sources. These may include the website of the supervisory authority of the respondent bank, for cross-checking identification data with the information obtained by the supervisor in the licensing process, or with regard to potential AML/CFT administrative sanctions that have been imposed on the respondent bank. This may also include public registries (see FATF guidance, paragraph 25).

22. In assessing whether to enter into a correspondent banking relationship, the correspondent bank should also consider relevant information on the jurisdiction in which the respondent operates, for instance from international bodies or other sources listed in paragraph 25 of the FATF guidance. Where deficiencies are identified in certain jurisdictions, correspondent banks should also take into account the corrective measures under way to strengthen the jurisdiction's AML/CFT controls, as well as efforts by domestic authorities to instruct respondent banks on how to strengthen their controls and mitigate ML/FT risks. This would be relevant especially where a correspondent bank is considering whether an existing correspondent banking relationship could be subject to additional monitoring or restrictions, rather than termination.

III. Assessment of the respondent bank's AML/CFT controls

23. All correspondent banking relationships should be subject to an appropriate level of due diligence following a risk-based approach, as presented above. The level of due diligence should be proportionate to the respondent bank's risk profile and consistent with paragraph 14 of the FATF guidance. Banks should not treat the CDD process as a "paper-gathering exercise" but as an essential step to support assessment of ML/FT risk, as described in paragraphs 9–11. This involves the correspondent bank assessing the respondent bank's AML/CFT controls on a risk-sensitive basis (for example, receiving a description of the respondent bank's AML/CFT procedures and systems, including sanctions screening, checking if the internal audit function regularly reviews the adequacy of the respondent bank's AML/CFT controls) consistent with the FATF guidance and the main body of the present guidelines. Based on the correspondent's own risk assessment, the information-gathering should be complemented by liaising

directly (eg by phone or videoconference) with the respondent bank's local management and compliance officer, or potentially by an on-site visit.

24. CDD information should also be reviewed and updated regularly, in accordance with the risk-based approach. The updating could be based on changes to risks associated with the respondent relationship. This information should be used to update the bank's risk assessment process.

IV. Customer acceptance and retention

25. The decision to enter into a correspondent banking relationship with a respondent bank should be approved by the relevant senior management[54] of the correspondent bank. When significant ML/FT risk factors emerge in an existing correspondent banking relationship, the correspondent should review the relationship. Following the review, the decision to continue the relationship with additional risk mitigation measures or to terminate it should be escalated to the relevant senior management.

26. Pursuant to the FATF standards (Recommendation 13), correspondent banks should refuse to enter into or continue correspondent banking relationships with "shell" banks (ie banks incorporated in a jurisdiction in which they have no physical presence and which is unaffiliated with a regulated financial group).[55] Correspondent banks should not enter into correspondent banking relationships if they are not satisfied, based on the information gathered or received, that the respondent bank is not a shell bank.

V. Ongoing monitoring

27. Correspondent banks should establish appropriate policies, procedures and systems to detect financial activity that is not consistent with the purpose of the services provided to respondent banks or any financial activity that is contrary to commitments that may have been concluded between the correspondent bank and the respondent bank. The level of ongoing monitoring should be commensurate with respondent banks' risk profiles.

28. Respondent banks should ensure that full and accurate originator and beneficiary information is included in payment messages sent to correspondent banks, in accordance with FATF Recommendation 16 and to enable correspondent banks to screen sanctions and monitor transactions.

29. If a correspondent bank decides to allow correspondent accounts to be used directly by third parties to transact business on their own behalf (payable-through accounts), it should conduct enhanced monitoring of these activities in line with the specific risks assessed. The correspondent bank should satisfy itself that the respondent bank has conducted adequate CDD on the customers with direct access to correspondent accounts and that the respondent bank can provide relevant CDD information upon request.

[54] The senior management consists of a core group of individuals responsible and accountable to the board for the sound and prudent day-to-day management of the bank; see Principle 4 in Basel Committee on Banking Supervision, *Corporate governance principles for banks*, July 2015.

[55] The FATF glossary defines "shell bank" as "a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence" means meaningful mind and management located within a country. The existence simply of a local agent or low level staff do not constitute physical presence".

30. As part of ongoing monitoring, if there are doubts after analysing unusual activity alerts generated by the monitoring process, the correspondent bank could issue a Request for Information on that particular transaction to the respondent bank.

31. Before considering withdrawing from a correspondent banking relationship, the correspondent bank may consider additional measures such as limiting the services provided, real-time monitoring, sample testing of transactions or on-site visits.

32. Senior management should be regularly informed of high-risk correspondent banking relationships and how they are monitored, particularly where risks are considered very high.

VI. The role of banks processing cross-border wire transfers

33. The Committee document *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* sets supervisory expectations concerning the respective roles of the originator's bank, the intermediary banks and the beneficiary's bank in processing a cross-border payment for a wire transfer. Although the document focuses on cover payments, most of the expectations apply more widely to all payment messages, as described below. Originating banks are responsible for using the right format for payment messages. They should require that information on the originator and beneficiary accompanies wire transfers, while others in the payment chain are required to monitor the payments they process based on this information. The Committee encourages all banks to apply high transparency standards, in full compliance with FATF Recommendation 16, and applicable national laws and regulations.

34. In particular, the quality of information provided in payment messages should be part of ongoing monitoring. Indeed, as mentioned in the Committee guidance on payment messages,[56] the correspondent bank as an intermediary should monitor the payment messages transmitted by the respondent bank for the purpose of detecting those which lack required originator and/or beneficiary information, including meaningless fields,[57] consistent with FATF Recommendation 16 and straight through processing. and verify the reliability of the respondent's controls, for instance via sample testing (ie a closer look at a few transactions to identify cases where they do not comply with the wire transfer information requirements).

35. Sample testing may also help the correspondent bank to adjust the level and type of monitoring, including the timing of ex post reviews.

36. The respondent bank, acting as the ordering financial institution, remains responsible for performing customer due diligence on the originator and must verify originator information for accuracy and maintain this information in accordance with local regulatory requirements implementing FATF Recommendation 16.

37. As recommended by the CPMI, the use of the LEI as additional information in payment messages should be possible on an optional basis in the current relevant payment messages (ie MT 202 COV and MT 103). Where available, the use of the LEI would facilitate the determination by the correspondent bank that the information in the message is sufficient to unambiguously identify the originator and beneficiary of a transfer.

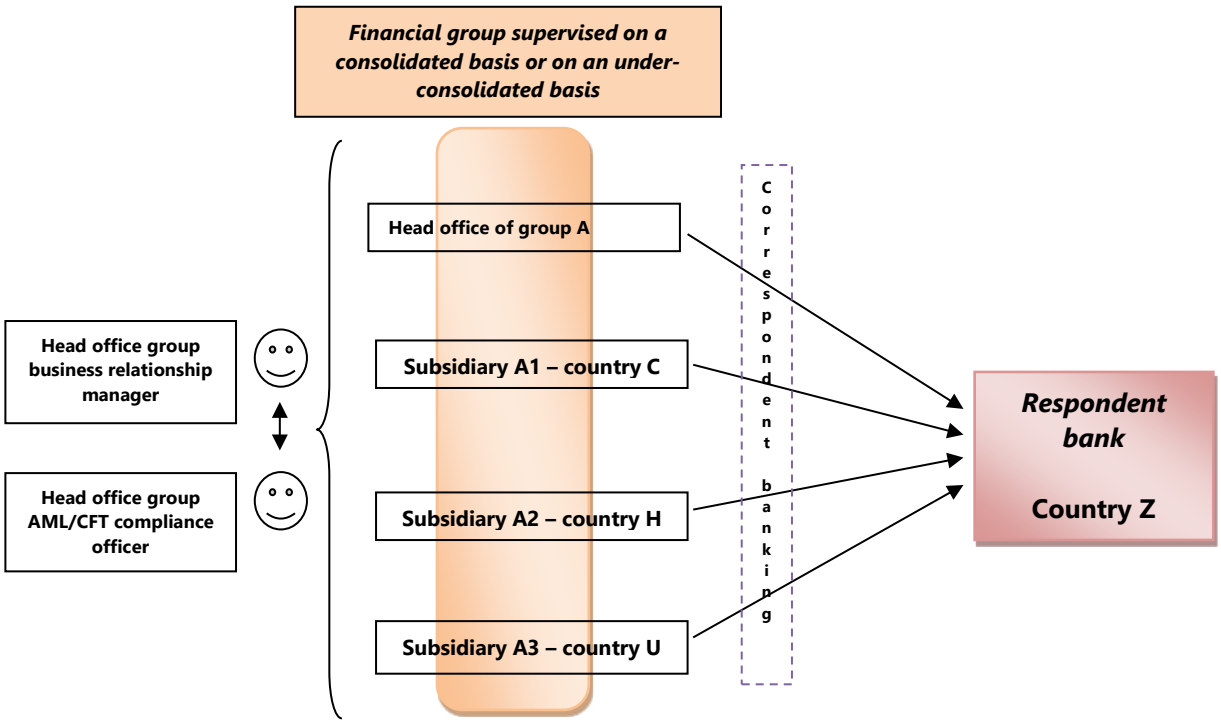
[56] See in particular paragraph 25 of Basel Committee on Banking Supervision, *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, May 2009.

[57] That is, information that makes no obvious sense, such as "one of my customers" or a pure string of characters.

VII. Group-wide and cross-border considerations

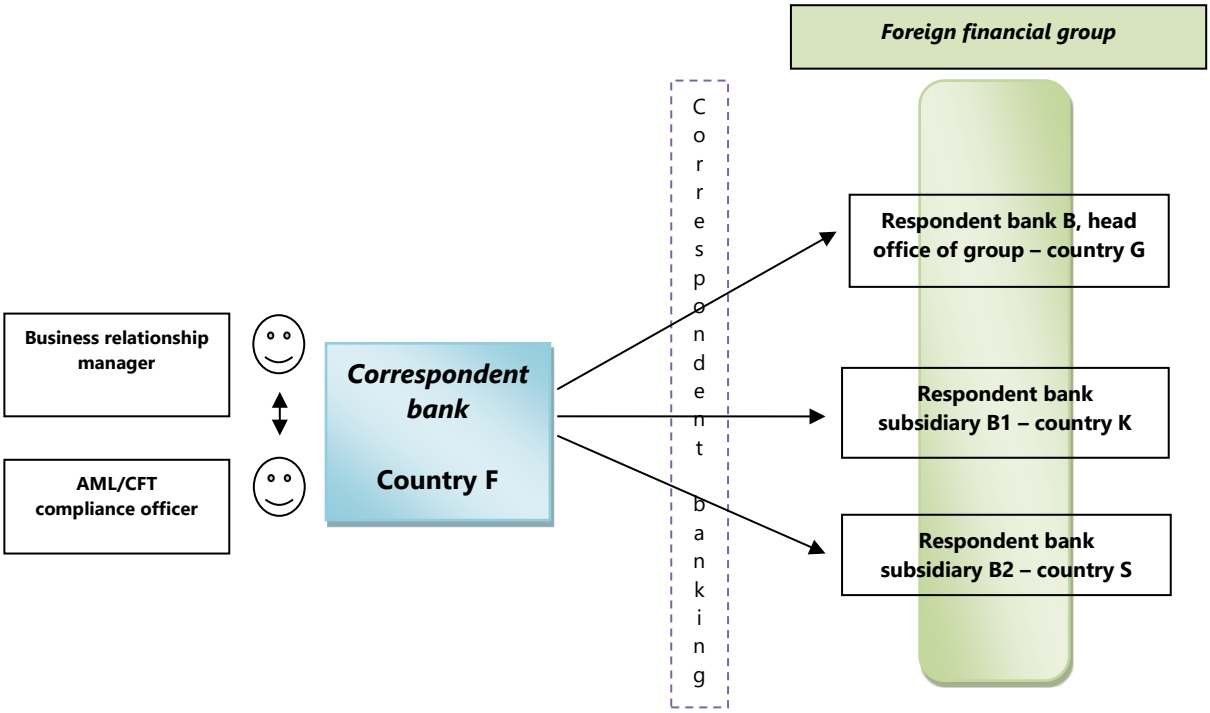
38. If a respondent bank has correspondent banking relationships with several entities belonging to the same group (case 1), the head office of the group should ensure that the assessments of the risks by the different entities of the group are consistent with the group-wide risk assessment policy. The group's head office should coordinate the monitoring of the relationship with the respondent bank, particularly in the case of a high-risk relationship, and make sure that adequate information-sharing mechanisms inside the group are in place.

Case 1



39. If a correspondent bank has business relationships with several entities belonging to the same group but established in different host countries (case 2), the correspondent bank should take into account the fact that these entities belong to the same group. Nevertheless, the correspondent bank should also independently assess the ML/FT risks presented by each business relationship.

Case 2



VIII. Risk management

40. Banks should establish specific procedures to manage correspondent banking relationships. Business relationships should be formalised in written agreements that clearly define the roles and responsibilities of the banking partners.

41. Including notice periods for terminating or limiting the business relationships in the terms and conditions governing the correspondent banking relationship is recommended as it should be part of the correspondent bank's risk management procedures. From the respondent bank's perspective, such notice periods should inform banks' business continuity plans.[58] As part of contingency planning for critical functions under operational risk management, a respondent bank may consider having more than one correspondent banking account for its payment services, where necessary for its continued operation.

42. Senior management should also be aware of the roles and responsibilities of the different services within the bank (eg business lines, compliance officers (including the chief or group AML/CFT officer), audit) pertaining to correspondent banking activities.

43. A bank's internal audit and compliance functions[59] have important responsibilities in evaluating and ensuring compliance with procedures related to correspondent banking activities. Internal controls should cover identification measures of the respondent banks, the collection of information, the ML/FT risk assessment process, ongoing monitoring of correspondent banking relationships and compliance with the duties to detect and report suspicions (about respondents and/or possible underlying subjects involved in the transactions).

[58] See in particular Principle 10 in Basel Committee on Banking Supervision, *Principles for the sound management of operational risk*, June 2011.

[59] See Basel Committee on Banking Supervision, *The internal audit function in banks*, June 2012, and BCP 26 on internal control and audit in *Core principles for effective banking supervision*, September 2012.

Annex 3

List of relevant FATF recommendations

FATF new recommendations (including their interpretative notes)
• R. 1: Assessing risks and applying a risk-based approach
• R. 2: National cooperation and coordination
• R. 9: Financial institution secrecy law
• R. 10: Customer due diligence
• R. 11: Record-keeping
• R. 12: PEPs
• R. 13: Correspondent banking
• R. 15: New technologies
• R. 16: Wire transfers
• R. 17: Reliance on third parties
• R. 18: Internal controls and foreign branches and subsidiaries
• R. 20: Reporting of suspicious transactions
• R. 26: Regulation and supervision of financial institutions
• R. 27: Powers of supervisors
• R. 35: Sanctions
• R. 40: International cooperation

Annex 4

General guide to account opening

I. Introduction

1. This annex is a general guide detailing the principles set out in the main body of these guidelines (paragraphs 35–41). This guide focuses on account opening. It is not intended to cover every eventuality, but rather to focus on some of the mechanisms that banks can use in developing an effective customer identification and verification programme. It also sets out the information that should be collected at the time of account opening and which will help the bank to develop and complete the customer risk profile.

2. For the purpose of this Annex, an account is defined as any formal banking or business relationship established by a bank to provide or engage in products, services, dealings, or other financial transactions. This includes demand deposits, savings deposits, or other transaction or asset accounts, or credit accounts or other extension of credit. In keeping with the scope of the original document issued by the Basel Committee in 2003, this guide only covers the opening of new accounts and not the conduct of occasional transactions.

3. The guidance set out in this annex is therefore intended to assist banks in defining their approach to account opening. It may be adapted for specific application by banks in respect of their AML/CFT policies and procedures, especially in developing sound customer risk profiles and by national financial supervisors seeking to further enhance the effectiveness of bank compliance with customer identification and verification programmes. Supervisors recognise that any effective customer identification/verification programme should reflect the risks arising from the different types of customer, types of banking product and the varying levels of risk resulting from a customer's relationship with a bank. Higher-risk customer relationships and transactions, such as those associated with politically exposed persons (PEPs)[60] or other higher-risk customers, will clearly require greater scrutiny than relationships and transactions associated with lower-risk customers. Therefore, the provisions in this guide should be read in conjunction with the main body of the guidelines, and in particular with the provisions related to assessing and understanding risks (see paragraphs 15–16 of the guidelines) and should be adapted for identified specific (higher- or lower-) risk situations.

4. Guidance and best practice established by national financial supervisors should be commensurate with the risks present in the jurisdiction; for this reason they will vary between countries. According to this risk-based approach, jurisdictions may allow simplified customer due diligence measures to be applied for lower-risk situations. For example, some jurisdictions have either taken or supported actions to encourage financial inclusion by promoting lower-risk financial products (such as an account with a limited set of services for specific types of customer). Conversely, in cases where there is a higher risk, banks should apply enhanced due diligence. Examples of such cases include the customer applying

[60] See in particular the *FATF Guidance on Politically Exposed Persons* (recommendations 12 and 22), www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

for specific products featuring non-face-to-face transactions, that allow anonymity of certain transactions,[61] or that are specifically vulnerable to fraud.

5. Similarly, banks' customer identification and verification policies and procedures will differ to reflect risks arising from the relevant categories of customers, products and services. In designing and implementing customer identification programmes and establishing a customer's risk profile, banks should take into account the risks arising from each type of financial product or service used by the customer as well as the delivery channel and the location.

6. According to the FATF standards,[62] banks should always identify customers and verify their identity.[63] When doing so, banks should be conscious that some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the validity of the document(s) presented, the verification requirement should be enhanced and the information provided by the customer should be verified through additional inquiries or other sources of information.

6bis. Supervisors recognise banks' growing use of external databases, such as KYC utilities or public registries for obtaining customer information. Different types of information may be contained in such databases and used by banks for different purposes, such as:

(a) helping identify the customer, by providing identification and, in some cases, beneficial ownership information;

(b) collecting information supporting the risk profile;

(c) in some cases, serving as an external source of verification.

Such databases may be used at different stages and for different types of customers, for instance at account opening for obtaining basic information, during the course of the relationship to update the information, or on an ongoing basis to assist banks with gathering information for their risk assessment process. Banks should take into account international standards, which require consideration of the reliability of the source,[64] and compliance with applicable national laws, which may prescribe certain customer identification or verification procedures. In the case of public registries, the banks should take into account the laws and procedures governing them. Banks should also be alert to the risk of identity theft, and take into account the fact that a database may help establish that a customer exists and gather information on that customer. However, the database may not necessarily confirm that the person the bank is dealing with is that customer.

6ter. In any case, the ultimate responsibility for CDD remains with the bank establishing the customer relationship. The level of risk associated with the customer and the KYC utility features will determine whether the bank needs to verify or corroborate the information provided by the utility and collect additional information, or take other measures. Therefore, when determining the extent to which they can use KYC utilities to support due diligence, banks should consider whether:

[61] Anonymous accounts are prohibited by the FATF but some products and new payment methods (certain prepaid cards, virtual currencies) could be higher risk, for example where they allow anonymous transactions,

[62] See recommendation 10.

[63] The extent and intensity of the process can nevertheless vary according to the risks involved. See *FATF Guidance on AML/CFT Measures and financial inclusion*, paragraph 61 and followings and *FATF RBA Guidance for the banking sector,* paragraph 63.

[64] For instance, FATF Recommendation 10 requires "(a) identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer. (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship." Interpretative Note to Recommendation 10 states "the relevant identification data may be obtained from a public register, from the customer or from other reliable sources".

(a) the utility clearly specifies the source of the information (eg the customer itself, a public registry) so that the bank can assess the adequacy of the source and whether it meets the level of confidence expected by the bank in the circumstances;

(b) the utility specifies the date of the last update and when the information was last confirmed with the source;

(c) the data quality is adequate, by assessing from time to time the reliability of the information in the utility (eg by verifying for a sample that the information matched the stated source at the stated date, with a frequency and depth depending on the extent to which the utility is itself subject to a transparent and independent data quality management programme).

7. The rest of this annex is divided into two sections covering different aspects of customer identification. Section II describes what types of information should be collected and verified for natural persons seeking to open accounts. Section III describes what types of information should be collected and verified for legal persons and legal arrangements.

II. Natural persons

A. Identification of individuals who are customers or beneficial owners or authorised signatories

8. For natural persons, the bank should collect the following information for identification purposes from the customer or any other available source:

Natural persons

Identification information

Table 1

At a minimum[a]	**Potential additional information (on the basis of risks)**
Legal name (first and last name);	Any other names used (such as marital name, former legal name or alias);
Complete residential address;[b]	Business address, post office box number, e-mail address and landline or mobile telephone numbers;
Nationality, an official personal identification number or other unique identifier;[b]	Residency status;[c]
Date and place of birth.[b]	Gender.[c]

(a) Not all this information may be required in lower-risk situations, when simplified due diligence can be applied. The list does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

(b) There are circumstances when this information is legitimately unavailable. This could prevent the clients from accessing formal banking services. If clients are allowed to access to formal banking services, banks should apply mitigating measures as provided for by their internal risk policies, in line with national laws. Such measures could include utilising alternative information or conducting appropriate monitoring.

(c) The collection of this information may be subject to national data protection and privacy regimes.

B. Information related to the customer's risk profile

9. When the account opening is the start of a customer relationship, further information should be collected with a view to developing an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

Natural persons

Risk profile's information — Table 2

Key attributes[a]	**Potential additional information (on the basis of risks)**
Occupation, public position held;	Name of employer, where applicable;
Income;	Sources of customer's wealth;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected;	Sources of funds passing through the account;
Financial products or services requested by the customer.	Destination of funds passing through the account.

(a) These key attributes are useful in establishing the first step of the customer's risk profile; they might not be required in lower-risk situations where simplified due diligence can be applied.

C. Verification of identity of natural persons

10. The bank should verify the identity of the customer established through information collected according to paragraph 8 using reliable, independently sourced documents, data or information. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should enable the bank to satisfy itself that it knows who the customer is. Examples of different verification procedures are given below. This list of examples is not exhaustive:

(a) Documentary verification procedures[65]

- confirming the identity of the customer or the beneficial owner from an unexpired official document (eg passport, identification card, residence permit, social security records, driver's licence) that bears a photograph of the customer;
- confirming the date and place of birth from an official document (eg birth certificate, passport, identity card, social security records);
- confirming the validity of official documentation provided through certification by an authorised person (eg embassy official, public notary);
- confirming the residential address (eg utility bill, tax assessment, bank statement, letter from a public authority).

In some jurisdictions, there may be other verification procedures of an equivalent nature that will provide satisfactory evidence of a customer's identity and risk profile.

[65] Even if not required nor necessary in all circumstances, given the availability of counterfeit and fraudulently obtained documents, a bank is encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

(b) Non-documentary verification procedures

- contacting the customer by telephone or by letter to confirm the information supplied, after an account has been opened (eg a disconnected phone, returned mail etc should warrant further investigation);
- checking references provided by other financial institutions;
- utilising an independent information verification process, such as by accessing public registers, private databases or other reliable independent sources (eg credit reference agencies).

11. Banks should verify that any person purporting to act on behalf of the customer is so authorised. If so, banks should identify and verify the identity of that person. In such a case, the bank should also verify the authorisation to act on behalf of the customer (a signed mandate, an official judgment or equivalent document).

D. Further verification of information on the basis of risks

12. Particular attention needs to be focused on those customers assessed as having higher-risk profiles.[66] Additional sources of information and enhanced verification procedures may include:

- confirming an individual's residential address on the basis of official papers, a credit reference agency search, or through home visits;
- prior bank reference (including banking group reference) and contact with the bank regarding the customer;
- verification of income sources, funds and wealth identified through appropriate measures; and
- verification of employment and of public positions held;
- personal reference (ie by an existing customer of the same bank).

13. If national law allows for non-face-to-face account opening, banks should take into account the specific risks associated with this method. Customer identification and verification procedures should be equally effective and similar to those implemented for face-to-face interviews. In particular, banks should (i) establish that the customer exists; and (ii) establish that the person the bank is dealing with is that customer.

14. As part of its broader customer due diligence measures, the bank should consider, on a risk-sensitive basis, whether the information regarding sources of wealth and funds or destination of funds should be corroborated.

III. Legal persons and arrangements and beneficial ownership

15. The procedures discussed previously in paragraphs 8–14 should also be applied to legal persons and arrangements. Banks should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure, with a view to establishing a customer risk profile.

[66] Without prejudice to FATF recommendations on PEPs and associated enhanced due diligence (see in particular Recommendation 12 within the FATF standards).

A. Legal persons[67]

16. The term legal person includes any entity (eg business or non-profit organisation, distinct from its officers and shareholders) that is not a natural person or a legal arrangement. In considering the customer identification guidance for the different types of legal persons, particular attention should be given to the different levels and nature of risk associated with these entities.

1. Identification of legal persons

17. For legal persons, the following information should be obtained for identification purposes:

Legal persons

Identification information

Table 3

At a minimum[a]	**Potential additional information (on the basis of risks)**
Name, legal form, status and proof of incorporation of the legal person;	
Permanent address of the principal place of the legal person's activities;	
Official identification number (company registration number, tax identification number);	Legal entity identifier (LEI) if eligible;[d]
Mailing and registered address of legal person;	Contact telephone and fax numbers.
Identity of natural persons who are authorised to operate the account. In the absence of an authorised person, the identity of the relevant person who is the senior managing official.	Identity of relevant persons holding senior management positions.
Identity of the beneficial owners[b] (according to relevant FATF standards and paragraph 13 of this annex); [c]	
Powers that regulate and bind the legal person (such as the articles of incorporation for a corporation).	

(a) Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The list does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

(b) The term "beneficial owner" is used in this annex in a manner consistent with the definition and clarifications provided in the FATF standards. For reference, the FATF defines a "beneficial owner" as 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.

(c) See *Interpretative note to recommendation 10* of the FATF. See also FATF, *Transparency and beneficial ownership*, October 2014, www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

(d) Subject to developments in the LEI project, this information may become required in the future.

[67] The FATF definition of "legal persons" refers to any entities other than natural persons that can establish a permanent customer relationship with a bank or otherwise own property. This can include companies, bodies corporate, foundations, *Anstalt*-type structures, partnerships, or associations and other relevantly similar entities.

2. Information for defining the risk profile of a customer which is a legal person

18. When the account opening is the start of a customer relationship, further information should be collected with a view to developing an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

Legal persons

Risk profile information — Table 4

At a minimum[a]	**Potential additional information (on the basis of risks)**
Nature and purpose of the activities of the legal entity and its legitimacy;	Financial situation of the entity;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Sources of funds paid into the account and destination of funds passing through the account.

(a) Not all this information may be required in lower-risk situations when simplified due diligence can be applied. The list does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

3. Verification of identity of legal persons

19. The bank should verify the identity of the customer established through information collected according to paragraph 17 using reliable, independent source documents, data or information. The bank should obtain:

- a copy of the certificate of incorporation and memorandum and articles of association, or partnership agreement (or any other legal document certifying the existence of the entity, eg abstract of the registry of companies/commerce);

20. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should allow the bank to satisfy itself that it knows the customer's identity. Examples of other verification procedures are given below. This list is not exhaustive.

(a) Documentary verification

- for established corporate entities – reviewing a copy of the latest financial statements (audited, if available).

(b) Non-documentary verification

- undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (eg lawyers, accountants);
- validating the LEI and associated data in the public access service;
- obtaining prior bank references;
- visiting the corporate entity, where practical;
- contacting the corporate entity by telephone, mail or e-mail.

In some jurisdictions, there may be other verification procedures of an equivalent nature that will provide satisfactory evidence of a customer's identity and risk profile.

4. Verification of identity of authorised signatories and of beneficial owners of the customer

21. Banks should verify that any person purporting to act on behalf of the legal person is so authorised. If so, banks should verify the identity of that person. This verification should entail verification of the authorisation to act on behalf of the customer (a signed mandate, an official judgment or equivalent document).

22. Banks should undertake reasonable measures to verify the identity of the beneficial owners, in accordance with the FATF definition referenced in Table 3 note b and the due diligence procedures for natural persons outlined in Section II above.

5. Further verification of information on the basis of risks

23. As part of its broader customer due diligence measures, the bank should consider, on a risk-sensitive basis, whether the information regarding financial situation and source of funds and/or destination of funds should be corroborated.

B. Legal arrangements[68]

1. Identification of legal arrangements

24. For legal arrangements, the following information should be obtained:

Legal arrangements
Identification information

Table 5

At a minimum[a]	**Potential additional information (on the basis of risks)**
Name of the legal arrangement and proof of existence;	Contact telephone and fax numbers if relevant;
Address, and country of establishment;	
Nature, purpose and objects of the legal arrangement (eg is it discretionary, testamentary etc);	Legal entity identifier (LEI), if eligible;[b]
The names of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (including through a chain of control/ownership);	The names of the relevant persons having a senior management position in the legal arrangement, if relevant, addresses of trustees, beneficiaries.

(a) Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The list does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

(b) Subject to developments in the LEI project, this information may be required in the future.

[68] The term "legal arrangements" is used in this annex consistently with the definition provided by the FATF standards. As a reminder, the FATF defines "legal arrangements" as express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include *fiducie*, *Treuhand* and *fideicomiso*.

2. Information for defining the risk profile of a customer which is a legal arrangement

25. When the account opening is the start of a customer relationship, further information should be collected with a view to develop an initial customer risk profile (see in particular paragraphs 37–39 of the main body of the guidelines):

Legal arrangements

Risk profile information

Table 6

At a minimum[a]	**Potential additional information (on the basis of risks)**
Description of the purpose/activities of the legal arrangement (eg in a formal constitution, trust deed);	Source of funds;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Origin and destination of funds passing through the account.

(a) Not all this information may be required in lower-risk situations where simplified due diligence can be applied. The list does not include other basic requirements that are not specifically related to AML/CFT requirements, such as collecting the signatures of the account holders.

3. Verification of identity of legal arrangement

26. The bank should verify the identity of the customer established through information collected according to paragraph 23, using reliable, independently sourced documents, data or information. The bank should obtain, at a minimum, a copy of documentation confirming the nature and legal existence of the account holder (eg a deed of trust, register of charities). Measures to verify the information produced should be proportionate to the risk posed by the customer relationship and enable the bank to satisfy itself that it knows the customer's identity.

27. Examples of other procedures of verification are given below. This list of examples is not exhaustive. In some jurisdictions, there may be other procedures of an equivalent nature which may be produced, applied or accessed as satisfactory evidence of a customer's identity and risk profile. It includes:

- obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- obtaining prior bank references;
- accessing or searching public and private databases or other reliable independent sources.

4. Verification of identity of authorised signatories and of beneficial owners of the legal arrangement

28. Banks should undertake reasonable measures to verify the identity of the beneficial owners of the legal arrangements, in accordance with paragraphs 10–11 above.

29. Banks should verify that any person purporting to act on behalf of the legal arrangement is so authorised. If so, banks should verify not only the identity of that person but also the person's authorisation to act on behalf of the legal arrangement (by means of a signed mandate, an official judgment or another equivalent document).

5. Further verification of information on the basis of risks

30. As part of its broader customer due diligence measures, the bank should consider, on a risk-sensitive basis, whether the information regarding source of funds and/or destination of funds should be corroborated.

C. Focus on specific types of customer

1. Retirement benefit programmes

31. Where an occupational pension programme, employee benefit trust or share option plan is an applicant for an account, the trustee and any other person who has control over the relationship (eg administrator, programme manager or account signatories) can be considered as beneficial owners and the bank should take steps to identify them and verify their identities.

2. Mutuals/friendly societies, cooperatives and provident societies

32. Where these entities are applicants for accounts, those persons exercising control or significant influence over the organisation's assets should be considered the beneficial owners and therefore identified and verified. This will often include board members as well as executives and account signatories.

3. Professional intermediaries

33. When a professional intermediary opens a customer account on behalf of a single customer that customer must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities. Where funds held by the intermediary are not co-mingled but "sub-accounts" are established which can be attributed to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the bank should look through to the beneficial owners. However, there may be circumstances – which should be permitted by law and set out in supervisory guidance – where the bank may not need to look beyond the intermediary (eg when the intermediary is subject to due diligence standards in respect of its customer base that are equivalent to those applying to the bank itself, such as could be the case for broker-dealers).

34. Where such circumstances apply and an account is opened for an open or closed-end investment company, unit trust or limited partnership that is subject to customer due diligence requirements which are equivalent to those applying to the bank itself, the bank should treat this investment vehicle as its customer and take steps to identify:[69]

- the fund itself;
- its directors or any controlling board where it is a company;
- its trustee where it is a unit trust;
- its managing (general) partner where it is a limited partnership;
- account signatories; and
- any other person who has control over the relationship eg fund administrator or manager.

35 Where other investment vehicles are involved, the same steps should be taken as in paragraph 34 where it is appropriate to do so. In addition, in cases when no equivalent due diligence standards apply to the investment vehicle, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.

[69] When the domestic AML/CFT requirements do not require all this information to be collected but, as a minimum, only one of the items mentioned, the account-opening bank should consider collecting the other items as additional information.

36. Intermediaries should be treated as individual customers of the bank and the standing of the intermediary should be separately verified by applying the appropriate methods listed in paragraphs 17-23 above.

Annex 5

Interaction and cooperation between prudential and AML/CFT supervisors

A. General provisions

1. Effective cooperation and exchange of information among prudential supervisors and AML/CFT supervisors that are responsible for banks (hereinafter "supervisors") are essential to address and mitigate ML/FT risk, to maintain the integrity of the banking system and to ensure the prudential soundness and stability of banks.

2. Supervisors should ensure efficient and effective cooperation between the prudential supervisory function and AML/CFT supervisory function (hereinafter "supervision"), regardless of the jurisdictional institutional arrangement for the respective functions. This cooperation may take place within a national authority undertaking multiple functions, between different national authorities responsible for different functions and also between different authorities in the cross-border context. This cooperation must not negatively impact the independence of either supervisory function in fulfilling its mandate. Moreover, this cooperation must not result in different supervisory functions unduly duplicating efforts.

3. Prudential supervision aims to ensure compliance by banks with prudential requirements, the safety and soundness of banks, and the stability of the banking system, including the authorisation of a bank, assessment of qualifying holding of bank shares, fit and proper tests of major shareholders, the board of directors and members of senior management, and ongoing assessment of the adequacy of the governance, organisational structure, risk management and internal control systems of a bank. For the purposes of these guidelines, the function that carries out prudential supervision over banks is referred to as the "prudential supervisor".

4. AML/CFT supervision in the banking sector aims to ensure compliance by banks with requirements for countering ML and/or FT and to assess banks' ML/FT risks and processes and internal control systems set up in order to mitigate those risks and to undertake supervisory actions on the basis of such assessments. For the purposes of these guidelines, the function that carries out the AML/CFT supervision over banks is referred to as the "AML/CFT supervisor". As AML/CFT supervisors have specialised expertise and knowledge of AML/CFT-related issues, the assessment of banks' ML/FT risk should be carried out by AML/CFT supervisors in the context of their ongoing AML/CFT supervision and considered in prudential supervision. AML/CFT supervisors should conversely consider in their assessment the knowledge and insights of the prudential supervisors, in particular on the overall risk management, internal controls and governance of the supervised entities.

5. Supervisors are expected to adopt practices, from applicable Financial Action Task Force (FATF) Recommendations and the Committee's principles and guidelines on the role and powers of supervisors (including their powers to impose sanctions) and information exchange, to appropriately consider ML/FT risks.

(1) Of the FATF recommendations relevant to supervisors, FATF Recommendation 27 (Powers of supervisors), Recommendation 35 (Sanctions) and Recommendation 40 and its Interpretative Note (Other forms of international cooperation) describe the roles and responsibilities of supervisors, their powers and authorities to enforce AML/CFT requirements that include a range of effective, proportionate and dissuasive sanctions, and the principles of information exchange and international cooperation among different public authorities, including prudential supervisors. Also for AML/CFT supervisors, FATF Recommendation 2 (National cooperation and coordination) is pertinent.

(2) Of the Committee's publications, the following are particularly relevant in the context of considering ML/FT risks in prudential banking supervision:

(a) *Core principles for effective banking supervision*, September 2012[70]

(b) *Corporate governance principles for banks*, July 2015[71]

(c) *Principles for effective supervisory colleges*, June 2014[72]

6. Deficiencies in banks' AML/CFT systems could have prudential consequences. For example, AML/CFT deficiencies could result in significant regulatory actions or criminal penalties that may lead to reputational damage affecting the bank's operations such as depositor outflows, loss of counterparties or loss of market access, including loss of correspondent banking relationships. Additionally, failures in AML/CFT may lead to the revocation of a banking licence or termination of deposit insurance in some jurisdictions. Supervisors should be aware that such AML/CFT deficiencies could be caused by or indicative of the bank's wider, overall failures in governance, organisational structure, risk management and compliance.

7. Information exchange should be created and maintained, to the extent permitted by applicable laws, in order to ensure that prudential supervisors have access to timely and appropriate information gathered during the AML/CFT supervisors' activities that could be relevant to prudential supervisors in considering ML/FT risks. Similarly, prudential supervisors should share with AML/CFT supervisors information gathered during their supervisory activities that could be relevant to the supervision of AML/CFT obligations and the assessment of ML/FT risks. This information exchange is limited to information that the requesting supervisor needs but does not have, and that the requested supervisor has available.

8. The cooperation and exchange of information between related functions should occur in conducting activities, including but not limited to:

(1) authorisation-related procedures of a bank, which include: licence applications for banks, qualifying holding assessments, and fit and proper tests both at the time of authorisation and on a continuing basis thereafter;

(2) ongoing supervision, including assessment of governance, risk management, and internal control systems of a bank, business model and profitability drivers, operational risks and compliance with AML requirements; and,

(3) enforcement actions[73] and/or revocation of a banking licence.

9. When considering ML/FT risks and assessing risk management for the purpose of activities as described in paragraph 8, prudential supervisors should also carefully consider the potential ML/FT risks identified by the AML/CFT supervisors that could stem from the international banking group structure and other cross-border activities, including the potential impact of a change of shareholders (also see Section B.1 (Licence of a bank) and Section B.2 (Assessment of major shareholders, acquisitions and increases of qualifying holdings)). In these guidelines, a bank also generally includes a banking group which is subject to consolidated supervision.

10. This annex provides principles, along with examples intended to provide practical information that supervisors should consider. The examples are not prescriptive and should be regarded as illustrative elements to provide further insight for applying and interpreting such issues. Supervisory practices

[70] Accessible at: www.bis.org/publ/bcbs230.pdf.

[71] Accessible at: https://www.bis.org/bcbs/publ/d328.pdf.

[72] Accessible at: https://www.bis.org/publ/bcbs287.pdf.

[73] See paragraph 22 for the definition of "enforcement actions".

provided in boxes highlight a range of practices, including some supervisory features specific to certain jurisdictions that may not be applicable to all.

11. All these principles and examples of practices should be considered according to a risk-based approach as set out in paragraphs 86 and 87 of these guidelines. Exchanges of information or other forms of cooperation should be proportionate to the risks and supervisory needs involved in each circumstance.

12. Under the risk-based approach for ML/FT, using the size of operations or profits/losses of a bank as the main or central ML/FT risk indicator would not be appropriate for concluding that a bank is low-risk, given that the ML/FT risk could also arise from relatively small parts or activities of a bank or a bank with a smaller asset size.

B. Cooperation and exchange of information in the authorisation process

13. The prudential supervisor is generally responsible for the authorisation processes of a bank (licence, qualifying holding assessments, and fit and proper tests) where applicable in conjunction with relevant regulatory authorities. It receives and assesses authorisation applications and should, as part of its assessment, involve the AML/CFT supervisor among other relevant parties. Therefore, the prudential supervisor should share with the AML/CFT supervisor appropriate information related to the application and receive information gathered or created in the exercise of the AML/CFT supervisor's functions, which is relevant in order to assess the application.

B.1 Licence of a bank

14. The prudential supervisor that is generally responsible for assessing the licence application of a bank should obtain information from the AML/CFT supervisor for the following purposes.

(1) The prudential supervisor should consider the exposure to ML/FT risks in its assessment of soundness of the business model of the bank. Examples include but are not limited to:

   (a) indications that the business model of a bank (including target customers, sectors, products and services, and distribution channels) presents a higher level of ML/FT risks, especially within a peer group; and

   (b) information on the jurisdiction where a bank is established or maintains significant business relationships, such as the nature and level of predicate offences to money laundering, the effectiveness of a jurisdiction's legal and judicial system, the scale and the level of risk of terrorist activities and groups in the jurisdiction, relevant ML/FT typologies identified by the jurisdiction's financial intelligence unit (FIU) and other public authorities and private entities, and the overall level of effectiveness of a jurisdiction's AML/CFT regime.

(2) The prudential supervisor should consider the bank's envisaged risk mitigation system, internal control system and adequacy of governance and organisational structures to properly manage ML/FT risks presented in the authorisation process. Examples include but are not limited to:

   (a) assessments of the adequacy of AML/CFT policies and procedures of the bank;

   (b) the organisation of the bank's AML/CFT function, including the adequacy of financial resources, staffing levels, training, and the information technology (IT) supporting the bank's AML/CFT unit; and

   (c) governance and management oversight of the bank's ML/FT risk exposures and risk management system.

B.2 Assessment of major shareholders, acquisitions and increases of qualifying holdings

15. The prudential supervisor is generally responsible for assessing major shareholders, proposed acquisitions or increase of a significant ownership.[74] The prudential supervisor should obtain information from the AML/CFT supervisor in order to consider potential effects of major shareholders and the acquisition or increases of holdings that qualify as significant ownership on the ML/FT risks of the bank, in particular in the context of cross-border banking groups, especially where the major shareholder or acquirer itself is subject to AML/CFT supervision.

(1) Thus, the prudential supervisor should consider whether:

(a) the major shareholder or proposed acquirer, which can be a natural person (also see Section B.3 (Assessment of natural persons)) or a legal person, is or has been involved in or associated with money laundering operations or attempts, whether or not this is directly or indirectly linked to the proposed acquisition;

(b) the major shareholder or proposed acquirer has been involved in or associated with or has carried out terrorist activities or terrorist financing, particularly if the proposed shareholder is subject to relevant enforcement actions and sanctions;[75] and

(c) the proposed transaction increases the ML/FT risks for the bank or impacts from the AML/CFT perspective on the business plan and the management and organisational structure of the bank.

(2) For the assessment of the major shareholders, the proposed transaction and the acquirer as described in above (1)(a) to (c), examples include but are not limited to:

(a) information on whether the major shareholder or proposed acquirer is established in or has significant business relationships with a country or territory identified by the FATF as having ML/FT strategic deficiencies;

(b) information regarding the sources of the funds used for the initial capital or proposed acquisition, including both the activity that generated the funds and the means through which they have been transferred, to assess whether this may give rise to an increased risk of ML/FT;

(c) information on whether the major shareholder or proposed acquirer itself is subject to AML supervision (eg bank); and

(d) information liable to give rise to questions on the increase of ML risk, such as relocations of headquarters to ML/FT high-risk countries, including countries that the FATF mutual evaluations identify as having significant deficiencies in their AML/CFT legal regulatory framework.

B.3 Assessment of natural persons

16. The prudential supervisor is generally responsible for assessing the fitness and properness of shareholders, including the ultimate beneficial owners and other persons that may exert significant influence, members of senior management, and members of the board of directors, at the time of authorisation of a bank as well as performing ongoing assessments. It should consult with the AML/CFT supervisor to obtain additional information, in order to ensure that the persons have a record of integrity and good repute, according to the essential criterion 7 of Principle 5 in *Core principles for effective banking supervision* and paragraph 51 in Principle 2 and paragraph 161 in Principle 13 of *Corporate governance*

[74] The ultimate beneficial ownership as set out in Core Principle 6 should also be considered in the context of this guideline for assessing the major shareholders.

[75] See paragraph 22 for the definition of enforcement actions and sanctions.

principles for banks, in particular that a bank is not controlled or owned by persons with links to significant ML/FT risks. Examples of relevant information to assess the suitability of the appointee include but are not limited to:

(1) past convictions or pending and ongoing prosecutions for a criminal offence and other relevant current or past measures taken by any regulatory or professional body for non-compliance with any relevant provisions. In this context, the stage of the proceedings, the materiality of the alleged non-compliance, the time that has elapsed since the past regulatory enforcement action or criminal penalty and the appointee's conduct since the misconduct, the personal involvement of the appointee and all other mitigating or aggravating factors, such as repeated infringement, are also relevant;

(2) any relevant findings from on-site and off-site supervision, from investigations or enforcement actions, to the extent that they relate to the proposed appointee; and

(3) other adverse information relevant to ML/FT risks regarding the appointee's conduct from credible and reliable sources to the extent possible, in particular when they are persistent.

Box 1

Example of practice: fit and proper assessment

In some jurisdictions, the fact that an individual or legal person is under investigation, indictment, enforcement action or prosecution for money laundering, sanctions violations or other similar offences as determined in these jurisdictions, could lead to further actions by the supervisor, requiring information about the underlying facts. Depending on the facts gathered and the legal framework, in some jurisdictions this could lead to a conditional approval of an application or to preventing an institution, individual or a group of individuals from engaging in certain banking activities (such as establishing or acquiring a bank, serving as executive management or engaging in new activities outside the approved business model). In some cases, the underlying facts could lead to a denial of approval without prejudice to the finalisation of the investigations of the other authorities.

C. Cooperation and exchange of information in ongoing supervision

17. Weaknesses or breaches in a bank's compliance with AML/CFT requirements could have significant legal, regulatory, criminal, reputational and financial impacts. ML/FT risks may affect the prudential analysis in the different components of its assessment of the bank's soundness. Therefore, the prudential supervisor should take into account the impact of the ML/FT risks by collecting and considering all relevant information identified by the AML/CFT supervisors. These prudential assessments should pay particular attention to the potential ML/FT risks that could stem from the cross-border banking group structure.

(1) ML/FT risks could impact the prudential supervisor's assessment of a bank's risk management, internal controls and governance. Examples include but are not limited to:

   (a) the level of personnel awareness of AML/CFT issues within the corporate culture as set out in *Corporate governance principles for banks*, particularly in relation to compliance records, the record of transparency and behaviour in relation with the relevant supervisors and FIUs;

   (b) the quality of the information given to the management and board of directors of the bank on AML/CFT topics, including information on major AML/CFT breaches, criminal or administrative sanctions, and risk indicators on AML/CFT activity;

   (c) the independence and the capacity of the risk management and internal control functions dedicated to the AML/CFT activities; and

(d) new adverse facts regarding shareholders (including beneficial owners), members of the management body and qualifying holders.

(2) ML/FT risks could impact the soundness of the business model. For example, information on transactions, business relationships and establishment in higher-risk countries could be relevant to determine this impact.

(3) ML/FT risks could impact the operational risk of a bank. For example, information on deficiencies regarding IT systems used by the bank to manage ML/FT risks could be relevant to raising awareness of the prudential supervisor about broader IT issues.

(4) ML/FT risks could impact the liquidity risk of a bank. For example, information on deposits received from countries with higher ML/FT risks or suspension of access to settlement services due to ML/FT issues could be relevant to the prudential supervisor's assessment of the soundness of the bank.

18. The information held by the AML/CFT supervisors could provide valuable insight for the exercise of prudential supervision. AML/CFT-related information in relation to a bank, its members of senior management and the board as well as any other information, findings or concerns could indicate weaknesses in the bank's prudential risk components, such as risk management, internal controls and governance. Besides the relevant information that is described in paragraph 17, the following examples of specific information sources held by the AML/CFT supervisor could be relevant for prudential supervision:

(1) AML/CFT topics identified by AML/CFT supervisors as priorities;

(2) assessment of ML/FT risks that could take into account component(s) directly linked to a prudential component;

(3) scheduled AML/CFT on-site examinations and the outcome of previous examinations;

(4) relevant AML/CFT reports from internal and external sources;

(5) AML/CFT supervisory measures. For example, supervisory measures taken against board members or members of senior management of the bank could have an impact on the prudential supervisor's assessment of the bank's governance framework. Supervisory measures that limit the bank's activity could have an impact on the business model. Financial penalties applied to the institution could have an impact on capital requirements or liquidity; and

(6) alerts related to ML/FT issues reported by whistleblowers.[76]

[76] See paragraph 32 in *Corporate governance principles for banks*, July 2015, for a description of whistleblowing principles.

Box 2

Example of practices

AML/CFT report

Some jurisdictions have required banks to prepare an AML/CFT risk assessment report and internal control report. This report is transmitted to senior management of the bank and to AML/CFT supervisors. It gives them relevant information regarding the ML/FT risks of the bank and corresponding mitigation measures. Such a document could be shared with prudential supervisors when relevant – that is, if a specific AML/CFT issue or an increased AML/CFT risk has been identified for an institution.

Impact of AML/CFT supervisor's assessment

Some jurisdictions have laws that require prudential supervisors to incorporate an explicit assessment of a bank's AML/CFT programme in making supervisory decisions such as reviewing various applications by banks. In those jurisdictions, AML programmes that are less than satisfactory may affect a bank's ability to expand, merge or acquire. As such, the information exchange on the AML/CFT supervisor's assessment could be useful in the licensing and ongoing supervision processes.

19. The information held by the prudential supervisor could be valuable for the exercise of AML/CFT supervision. An analysis of prudential information regarding a bank, its members of senior management and the board as well as any other information, findings or concerns could be relevant to the AML/CFT supervisory assessment of the bank's ML/FT risk components, such as the bank's internal control systems to identify and manage ML/FT risks.

(1) Prudential information about a bank's governance and risk management could be relevant for the AML/CFT supervisor. Examples of relevant information include but are not limited to:

   (a) the ownership and corporate structure of a bank, and the level of complexity and transparency of its organisation and structure;

   (b) deficiencies detected in governance and management oversight of a bank, as it could generally impact the effectiveness of AML/CFT systems at the bank. In particular, a lack of involvement of the risk management, control and compliance functions in important managerial decisions could signal weaknesses in the AML/CFT function;

   (c) prudential supervisory measures taken in relation to the governance framework and rejections of acquisitions of qualified holdings, proposed members of senior management or members of the board on the grounds of operational and reputational risk; and

   (d) concerns regarding the integrity and good repute of senior managers, members of the management body and significant shareholders (including beneficial owners).

(2) Prudential information about the business model could be relevant for AML/CFT supervision. This includes information on prudential supervisory measures such as restrictions to operations, including the establishment or provision of certain services.

(3) Prudential information on operational risks such as deficiencies in a bank's IT system or lines of defence[77] could be relevant for the AML/CFT supervisor.

20. Prudential information that could be relevant and provided to the AML/CFT supervisor could be obtained from the following sources:

[77] See *Principles for the sound management of operational risk*, June 2011 (available at https://www.bis.org/publ/bcbs195.pdf), for a description of the three lines of defence.

(1) information from on-site examinations, off-site surveillance and enforcement actions that is related to ML/FT risks; and

(2) information gathered during the authorisation, licensing or passporting process that is related to ML/FT risks.

Box 3

Example of practices

Practice concerning access to sources

In some jurisdictions, where AML/CFT supervision and prudential supervision are conducted by the same authority, AML/CFT examiners have access to current and historical information and documents about examinations conducted by the prudential supervisor.

Prudential-AML/CFT coordinated examination processes

In some countries, where prudential supervision and AML supervision are conducted by the same authority, examiners with a range of assignments and specialties, including AML/CFT, can be on-site at the same time. By examining the bank for safety and soundness and AML/CFT compliance at the same time, examiners are able to discuss all aspects of the bank's operations as well as evaluate the bank's policies, procedures and processes together.

A common example of the beneficial synergy between prudential and AML/CFT supervisors would include the review of a merger between two institutions. A concurrent review might highlight dissimilar business models, distinct credit underwriting standards and different customer types. The acquiring bank may be unfamiliar with certain products and services acquired, and may not have the experience or infrastructure (technology or staff) to adequately monitor the different customer types for suspicious activity. Without both disciplines discussing the merger, some of the important details could be overlooked.

D. Cooperation and exchange of information regarding enforcement actions

21. This section establishes principles for sharing information on enforcement actions or sanctions between prudential and AML/CFT supervisors at domestic and international levels.

22. Prudential and AML/CFT supervisors should share relevant information with domestic and international counterparts, in a timely manner and as appropriate consistent with applicable legal and other requirements, regarding pending or imposed enforcement actions or sanctions on a financial institution that are relevant and necessary for the supervisory function of the counterpart. The sharing of information may depend on the type and severity of the supervisory action, the confidentiality requirements of the investigation, whether the international counterpart provides reciprocal assistance, and whether such sharing would prejudice the interests of the home jurisdiction of the prudential regulator. Communication where appropriate should include sufficient detail regarding the nature of the AML/CFT deficiencies involved to enable each supervisor to assess the impact of those deficiencies on the supervised institution, in the context of the supervisor's mandate and function. It should occur as early and often as possible in order to manage the potential impact of the enforcement action or sanctions on financial stability (eg such as capital adequacy and liquidity concerns, revocation of banking licences or authorisations, termination of deposit insurance, or significant curtailment of activities).

23. For the purpose of this guideline, the term "enforcement action" or "sanctions" refers to the range of civil or administrative actions, often public, imposed on financial institutions by supervisors for significant non-compliance with AML/CFT requirements. The focus of this guideline is on banking supervision, so that the terms "enforcement actions" or "sanctions" do not include actions imposed on

financial institutions by law enforcement authorities for criminal violations of AML/CFT requirements or actions imposed by other non-bank supervisory government agencies.[78, 79] Moreover, in this guideline, the use of the term "enforcement actions" or "sanctions" is separate and distinct from "asset seizures and freezes" or "targeted financial sanctions", as defined by the FATF.

(1) In some countries, enforcement actions or sanctions can include civil or administrative money penalties, corrective action, and supervisory actions which may result in the curtailment of certain banking activities due to significant AML/CFT issues.

(2) Separately, in certain jurisdictions supervisors may have the authority to assess civil or administrative money penalties against bank insiders and may also remove and prohibit individuals from participating in the affairs of a bank (including employment).

(3) Enforcement actions or sanctions can also impact a financial institution's ability to engage in certain activities and expansion, since the effectiveness of a financial institution's AML/CFT efforts may be expressly required to be considered by a jurisdiction's laws and regulations on banking applications and licensing. In some jurisdictions, in addition to a criminal action concerning certain violations for money laundering, supervisors may consider additional actions such as the revocation of an institution's banking charter/licence or termination of the institution's deposit insurance. There may be other situations where a supervisor may consider AML/CFT related violations as grounds for the appointment of an administrator or receiver.

Box 4

Example of practice: enforcement action information exchange in the cross-border context

In some host jurisdictions, prudential supervisors share information with their foreign home supervisors about deficiencies in AML/CFT compliance and the possible consequences. Once imposition is imminent, they then follow up with information about pending enforcement actions. The host prudential supervisors also may share information with the home supervisors, as they are able and as appropriate, about possible non-supervisory (eg criminal) sanctions, as well as relevant information about possible consequences of the enforcement actions (eg the impact of the enforcement actions on possible future expansion and acquisition activities of the bank involved).

E. Mechanisms for cooperation, information exchange and confidentiality treatment

E.1 Channels of cooperation and information exchange at the jurisdictional and international level

24. Supervisors should establish and maintain official channels to facilitate and structure ongoing dialogue, information exchange and cooperation between prudential and AML/CFT supervisors, at the jurisdictional and international level, and use those channels effectively to inform relevant stages of the supervisory process. Examples of such channels between supervisory authorities include bilateral or multilateral exchanges with or without a memorandum of understanding (MoU), prudential supervisory colleges and dedicated AML/CFT colleges.

[78] Nevertheless, enforcement actions or sanctions by authorities other than AML/CFT supervisors can be relevant for the exercise of prudential supervision. Thus, a similar information exchange process is in principle beneficial. Such cooperation should not impinge on ongoing inquiries, investigations or proceedings in accordance with the criminal or administrative law.

[79] The term "non-bank supervisory government agencies" refers to authorities that have AML/CFT-related enforcement powers but are not supervisors of banks.

25. At the jurisdictional level, prudential and AML/CFT supervisors should consider the following items presented as examples below when putting in place mechanisms to ensure the exchange of information and cooperation in a timely and effective manner:

(1) Where prudential and AML/CFT supervisors are part of the same supervisory authority, internal processes should clearly establish, when the teams in charge are different, the need to work together and exchange information, both proactively and upon request, whilst maintaining the independence of each function.

(2) Where prudential and AML/CFT supervisors are not part of the same supervisory authority, both supervisors should consider putting in place an Agreement or MoU[80] that sets out, for example:

(a) In relation to the exchange of information:

i. the type of information that can or should be exchanged;

ii. situations where the request for information may be refused;

iii. the modalities of information exchange (including means of communication and, where applicable, the language used in the information communication);

iv. confidentiality and data protection provisions (including acceptable uses, by the requesting or receiving party, of the information obtained, including the ability for onward transmission of information to a third party at home or abroad); and

v. the legal basis for information exchange.

(b) In relation to cooperation:

i. areas in which cooperation is possible, and the purpose of such cooperation;

ii. a mechanism to agree on the manner to cooperate effectively in cases where several authorities have an interest in investigating the same entity, and where there is a risk that one investigation might prejudice the other. This could also set out which authority will take priority or take the lead in those cases and under which circumstances; and

iii. the legal basis for cooperation.

(c) A mechanism to attempt to resolve any disagreements among supervisory authorities, as necessary.

26. At the international level, in respect of banks operating across borders, prudential and AML/CFT supervisory authorities should put in place and maintain mechanisms to ensure the exchange of information and cooperation across borders in a timely and effective manner. To that end, supervisors should consider taking into account the mechanisms described in paragraph 25(2). As part of this, supervisory authorities should consider whether the use of either, or a combination of, colleges of prudential supervisors ("prudential colleges"), AML/CFT colleges, where they are provided for, and bilateral relationships effectively meets their supervisory needs.

(1) Prudential colleges can discuss prudential implications of AML/CFT issues and their impact on prudential objectives as part of the prudential college meetings or in AML/CFT substructures that can be set up as part of the prudential college. Addressing prudential implications of AML/CFT issues in the prudential college's context establishes a clear link between prudential and AML/CFT supervisors. To support informed decision-making, prudential colleges should consider inviting

[80] For example, the ECB and numerous AML/CFT authorities responsible for the AML/CFT supervision of credit and financial institutions in the member states of the European Economic Area have signed an agreement including most of the below-listed items, which are accessible at:

https://eba.europa.eu/documents/10180/2545547/Agreement+between+CAs+and+the+ECB+on+exchange+of+information+on+AML.pdf/e83dd6ee-78f7-46a1-befb-3e91cedeb51d.

AML/CFT supervisors to participate in prudential colleges as members or observers. For example, the lead supervisor of the AML/CFT college, where it is provided for, may be invited to prudential colleges. This would avoid a situation where, while focusing only on prudential objectives and considerations, the AML/CFT issues are considered only after ML/FT risks have already crystallised.

(2) AML/CFT colleges, where they are provided for, establish a formal framework for cooperation and information exchange amongst supervisors with an AML/CFT remit. Bringing together AML/CFT supervisors in this way ensures that ML/FT risks associated with a particular bank or group operating in multiple jurisdictions can be identified and effectively mitigated before they have crystallised. To be effective, AML/CFT colleges nevertheless have to build strong links with prudential supervisors and their prudential college counterparts where they are provided for, to ensure that information regarding ML/FT risks that are relevant from a prudential perspective, and prudential risks that are relevant from an AML/CFT perspective, is exchanged and can be acted upon in a timely fashion. To that effect, prudential supervisors could be members of these colleges, or be invited as observers. AML/CFT colleges might be used as a mechanism to improve the effectiveness of the AML/CFT supervision of international banking groups through collaborative work among members and observers while recognising national regulatory specificities of the AML/CFT frameworks.

(3) Where such mechanisms as set out above as part of a prudential college or an AML/CFT supervisory college have not yet been put in place, prudential and AML/CFT supervisors should put in place and maintain mechanisms to ensure the bilateral exchange of information and cooperation on a cross-border basis in a timely and efficient manner. Supervisors should consider referring to the mechanisms described in paragraph 25(2).

Box 5

Example of practice: AML/CFT supervisory colleges

AML/CFT and prudential legislation in the European Union (EU) establishes an obligation for competent authorities to cooperate and exchange information, but it does not set out in detail how this should be achieved. In the absence of a common framework, cooperation and information exchange between prudential and AML/CFT supervisors for the purposes of AML/CFT supervision can sometimes be difficult.

To address this, the European Supervisory Authorities (ESAs) issued *Guidelines on supervisory cooperation and information exchange* in December 2019.[81] These Guidelines lay down the rules on the establishment and operation of AML/CFT colleges.

As is the case with prudential colleges, AML/CFT colleges serve as a forum for collaboration and exchange of information. They support the development of a common understanding, by all supervisors, of the ML/FT risks associated with a bank or financial institution and inform the AML/CFT supervision of that bank or financial institution. For example, the Guidelines set out how AML/CFT supervisors can use AML/CFT colleges to adopt a common approach and agree on coordinated actions.

The Guidelines provide that AML/CFT colleges be set up for all banks and financial institutions that operate in at least three EU member states. All EU AML/CFT supervisors involved in the supervision of the bank or financial institution for which a college is set up are permanent members of that college.

EU prudential supervisors and the AML/CFT supervisors of non-EU countries where the institution operates are invited to participate in the AML/CFT college as observers. Prudential supervisors from non-EU countries and the FIU of the EU member state where the lead supervisor is located may be invited to participate as observers as appropriate.

All observers have to be subject to confidentiality rules equivalent to those in force in the EU. They are expected actively to participate, including by exchanging information within the AML/CFT college. Observers that are prudential supervisors are further expected to take action to ensure that information from AML/CFT college meetings is shared with colleges of prudential supervisors and acted upon as appropriate.

FIUs from other jurisdictions, as well as other relevant persons, may be invited to participate in the AML/CFT college on an ad hoc basis as necessary.

E.2 Processes of cooperation and information exchange

27. Prudential and AML/CFT supervisors should exchange information periodically and when necessary as relevant for their respective tasks, taking into account the mechanisms described in paragraph 25(1) and 25(2), as appropriate.

28. In the case of a request for information, the requested supervisor should determine whether the requested information is available and can be provided under the applicable regulations and laws.

(1) Where the request cannot be fulfilled in part or in whole – for example, because the requested information is not available or the fulfilment of the request would result in a breach of laws or regulations – the requested supervisor should cooperate to the fullest extent possible and consider whether it can provide other assistance. Also in such a case, the requested supervisor should inform the requesting party of the decision, explain why it cannot exchange information and consider including advice on how else it might be able to assist.

[81] The ESAs Guidelines are accessible at: https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/jc-guidelines-on-cooperation-and-information-exchange-for-aml/cft-supervision-purposes#pane-289.

(2) Where the request can be fulfilled, the supervisor should endeavour to exchange the requested information within the time set in the request. If providing data within the requested time is impossible or excessively burdensome, the supervisor should offer an alternative delivery date on which the requesting and requested parties can agree.

29. Prudential and AML/CFT supervisors should consider whether, and if so, in which situations, to cooperate, for example by carrying out coordinated or joint inspections. Such inspections could take place among prudential and AML/CFT supervisors of the same jurisdiction and also among home and host supervisors in the respective jurisdictions in accordance to the cooperation arrangements among relevant supervisors and the applicable regulations and laws.

30. When deciding whether to cooperate, supervisors should consider:

(1) the nature and level of the ML/FT risk associated with the bank;

(2) the focus of the proposed cooperation, including a bank's compliance with specific legal or regulatory provisions, such as legal and regulatory requirements to conduct customer due diligence (CDD) or to report suspicious transactions, or specific ML/FT risks that have been identified; and

(3) the availability and planned allocation of supervisory resources.

31. When taking the decision to cooperate, supervisors should consider setting out in writing, at a minimum:

(1) which supervisory authority is responsible for coordinating actions, if appropriate;

(2) an action plan, including the nature and type of actions that can be taken by each participating supervisor, the timing of the work to be undertaken by each participating supervisor and the modalities of information exchange, including the sharing of information gathered during, and as a result of, the cooperation; and

(3) the options for coordinated follow-up, if any, including, where applicable, cooperation in relation to an enforcement action.

E.3 Cooperation and information exchange between supervisors and third parties

32. Information relevant to both prudential and AML/CFT supervisors may be held by third parties, domestically or in another jurisdiction (eg a jurisdiction's FIUs or law enforcement agencies). In line with FATF Recommendation 2, in those cases, supervisors should ensure that they put in place and maintain effective channels to cooperate and exchange information at both operational and policy levels, to the extent that this is relevant, in a risk-based manner.

33. Where enforcement actions are imposed by law enforcement authorities or other public authorities, such as FIUs, supervisors should endeavour to share timely and relevant information with their domestic and international counterparts, within the scope of applicable law and investigative confidentiality requirements. Such cooperation should not impinge on ongoing inquiries, investigations or proceedings in accordance with criminal or administrative law.

34. Given the importance of cooperation with law enforcement agencies, FIUs and other relevant non-supervisory AML/CFT agencies for an effective supervision, both prudential and AML/CFT supervisors should consider taking measures to facilitate cooperation and information exchange with all relevant third parties, for example by entering into an Agreement or MoU such as the mechanisms described in paragraphs 24 to 26.

E.4 Confidentiality and data protection provisions

35. When putting in place mechanisms to ensure the exchange of information and cooperation among authorities in line with paragraphs 24 to 26 and 32, supervisors should include, to the extent legally possible, confidentiality and data protection provisions as follows:

(1) A confidentiality clause, specifying that all the information exchanged under such arrangement can only be used for supervisory purposes or purposes linked to the AML/CFT responsibilities of the party receiving the information. As part of this, authorities should consider specifying in the arrangement that the exchanged information must be classified as "confidential", and that requirements should be adopted in order to ensure the appropriate, high level of security for transmission and storage of information.

(2) Measures governing the dissemination of information to third parties. Dissemination of information obtained from other authorities should be subject to prior authorisation by the requested authority, unless the requesting authority is under a legal obligation to disclose or report the exchanged information, and vice versa; in such cases, the requesting authority should promptly inform the requested authority of this obligation to the extent permitted by law.

(3) Data protection provisions. When required by applicable laws, parties to the agreement should be allowed to exchange sanitised data; in the case of information related to ongoing law enforcement investigations or suspicious transaction reporting, the transmission of sanitised data should be authorised by the originating authorities.

(4) Safeguards to protect the identity of whistleblowers where the information exchanged is gathered from whistleblowing.