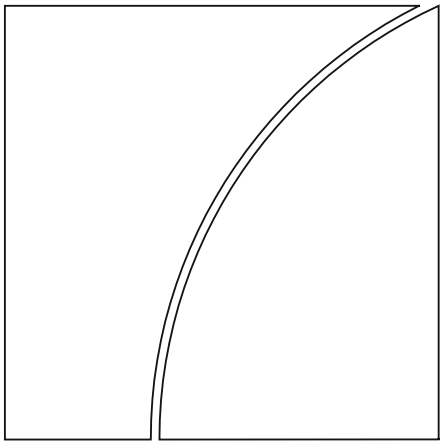
Basel Committee
on Banking Supervision



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

January 2014

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 92-9131-313-0 (print)

ISBN 92-9197-313-0 (online)

Contents

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

[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.

worldwide with the purpose of enhancing financial stability".[4] Sound ML/FT risk management has particular relevance 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]
- *Principles for enhancing corporate governance*, October 2010[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]

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 services (see Annex 2). Despite their importance and relevance, other specific risk areas such as

4 See Basel Committee on Banking Supervision, *Charter*, January 2013, accessible at www.bis.org/bcbs/charter.pdf.

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: www.bis.org/publ/bcbs176.pdf.

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

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

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.[11]

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.[12] 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.[13] 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.

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.

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".[14] 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.

[11] 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.

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

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

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

1. Assessment, understanding, management and mitigation of risks

(a) Assessment and understanding of risks

15. Sound risk management[15] 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,[16] 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.[17] 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 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.

15 See in particular BCP 15 in *Core principles for effective banking supervision*, September 2012 as well as Principle 6 in *Principles for enhancing corporate governance*, October 2010.

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

17 See, in particular, *The internal audit function in banks*, June 2012; *Principles for enhancing corporate governance*, October 2010*; Compliance and the compliance function in banks*, April 2005.

(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.[18] 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 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.

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

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.[19] 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*[20] 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 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.

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

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

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[21] 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.[22] In accordance with the FATF standards, banks should identify customers and verify their identity.[23]

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[24] 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.[25] 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

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

22 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.

23 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.

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

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

collected. Therefore, a bank 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.[26] 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.

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

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).

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[27] 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

[27] 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.

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.

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.[28] 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.

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

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.

(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.[29] 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

[29] 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.

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,[30] 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.

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).

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

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.[31] 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

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

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 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.[32] 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; [33] (ii) evaluate the adequacy of the bank's risk assessment based on the jurisdiction's national risk assessment(s); [34] (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

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

[33] 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.

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

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.[35] 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 that are considered to have strategic AML/CFT deficiencies or that do not comply with international AML/CFT standards,[36] 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[37] 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

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

[36] 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.

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

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 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.

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.[38] 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[39] 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

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

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

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 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) Third parties 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[40] allow 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

[40] See Recommendation 17 in the FATF Standards.

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 and 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.

15. 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.

16. 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 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")".

2. Used by banks throughout the world, correspondent accounts enable respondent banks to conduct business and provide services[41] that they cannot offer directly (because of the lack of an international network). Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence.

3. The correspondent bank processes/executes transactions for customers of the respondent. The correspondent bank generally does not have direct business relationships with the customers of the respondent bank, who may be individuals, corporations or financial services firms. The customer of the correspondent bank is the respondent bank.

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

II. Correspondent banking ML/FT risk assessment – information gathering

5. Banks that undertake correspondent banking activities should conduct an appropriate assessment of the ML/FT risks associated with correspondent banking activities and consequently apply appropriate customer due diligence (CDD) measures.

6. Correspondent banks should gather sufficient information, at the beginning of the relationships and on a continuing basis after that, about their respondent banks to fully understand the nature of the respondent's business and correctly assess ML/FT risks on an ongoing basis.

7. Factors that correspondent banks should consider include:

(a) the jurisdiction in which the respondent bank is located;

(b) the group to which the respondent bank belongs, and the jurisdictions in which subsidiaries and branches of the group may be located;

[41] 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" as mentioned in the FATF Glossary.

(c) information about the respondent bank's management and ownership (especially the presence of beneficial owners or PEPs), its reputation,[42] its major business activities, its customers and their locations;

(d) the purpose of the services provided to the respondent bank;

(e) the bank's business including target markets and customer base;

(f) the condition and quality of banking regulation and supervision in the respondent's country (especially AML/CFT laws and regulations);

(g) the money-laundering prevention and detection policies and procedures of the respondent bank, including a description of the CDD applied by the respondent bank to its customers;

(h) the ability to obtain identity of any third-party entities that will be entitled to use the correspondent banking services;

(i) the potential use of the account by other respondent banks in a "nested" correspondent banking relationship. [43]

8. Information on the AML/CFT policies and procedures may rely on any questionnaire filled by the respondent or on publicly available information provided by the respondent (such as financial information or any mandatory supervisory information).

III. Customer due diligence requirements

9. If correspondent banks fail to apply an appropriate level of due diligence to correspondent banking relationships, they may find themselves holding and/or transmitting money linked to illegal activity.

10. All correspondent banking relationships should be subject to an appropriate level of CDD. Banks should not treat the CDD process as a "paper-gathering exercise" but as a real assessment of ML risk. The gathering of information should be finalised, if necessary, based on meeting with the local respondent bank's management and compliance officer, regulator/supervisor, financial intelligence units and relevant governmental agencies.

11. CDD information should also be reviewed and updated on a regular basis, in accordance with the risk-based approach. This information should be used to update the bank's risk assessment process.

IV. Customer acceptance

12. The decision to accept (or continue) a correspondent banking relationship should be approved at senior level of the correspondent bank.

[42] Reputation may include civil, administrative or criminal actions/sanctions (fines, blame etc) that have been pronounced by any court or supervisory authority.

[43] Nested 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. Information may be provided by FATF mutual evaluation reports and statements on jurisdictions identified by the FATF as either being subject to countermeasures or having strategic AML/CFT deficiencies. Mutual evaluation reports by FATF-style regional bodies (FSRBs) may also provide such information. Any publicly available information from competent national authorities may also be used by banks. The fact that a country is subject to restrictive measures, particularly if there are prohibitions on providing correspondent banking services, should be taken into account. Correspondent banks should pay particular attention when establishing or continuing relationships with respondent banks located in jurisdictions that have deficient AML/CFT standards or have been identified as being "non-cooperative" in the fight against money laundering and terrorism financing.

14. Correspondent banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (ie shell banks).

V. Ongoing monitoring

15. A correspondent bank should establish appropriate policies and procedures to be able to detect any activity that is not consistent with the purpose of the services provided to the respondent bank or any activity that is contrary to commitments that may have been concluded between the correspondent and the respondent.

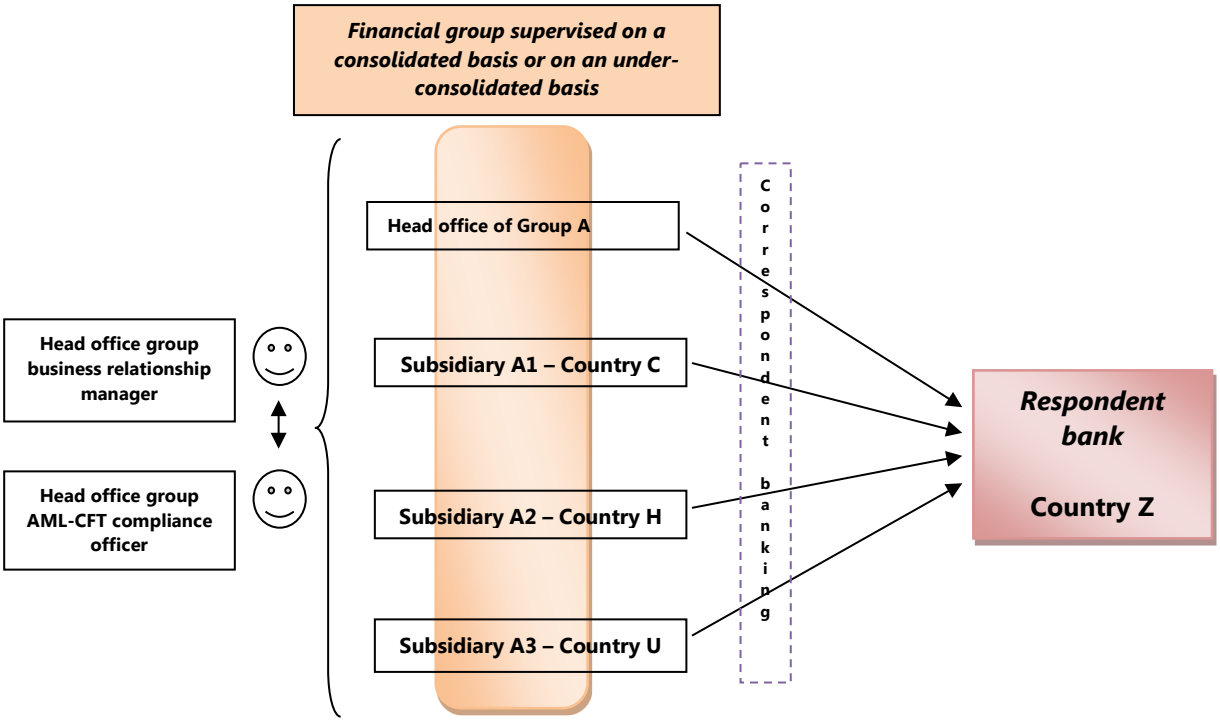
16. If a correspondent bank decides to allow correspondent accounts be used directly by third parties to transact business on their own behalf (eg payable-through accounts), it should conduct enhanced monitoring of these activities in line with their specific risks. The correspondent bank should verify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

17. Senior management should be regularly informed of high-risk correspondent banking relationships and how they are monitored.

VI. Group-wide and cross-border considerations

18. If a respondent bank has correspondent banking relationships with several entities belonging to the same group[44] (case 1), the head office of the group should pay particular attention that the assessments of the risks by the different entities of the group are consistent with the group-wide risk assessment policy. The head office of the group 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.

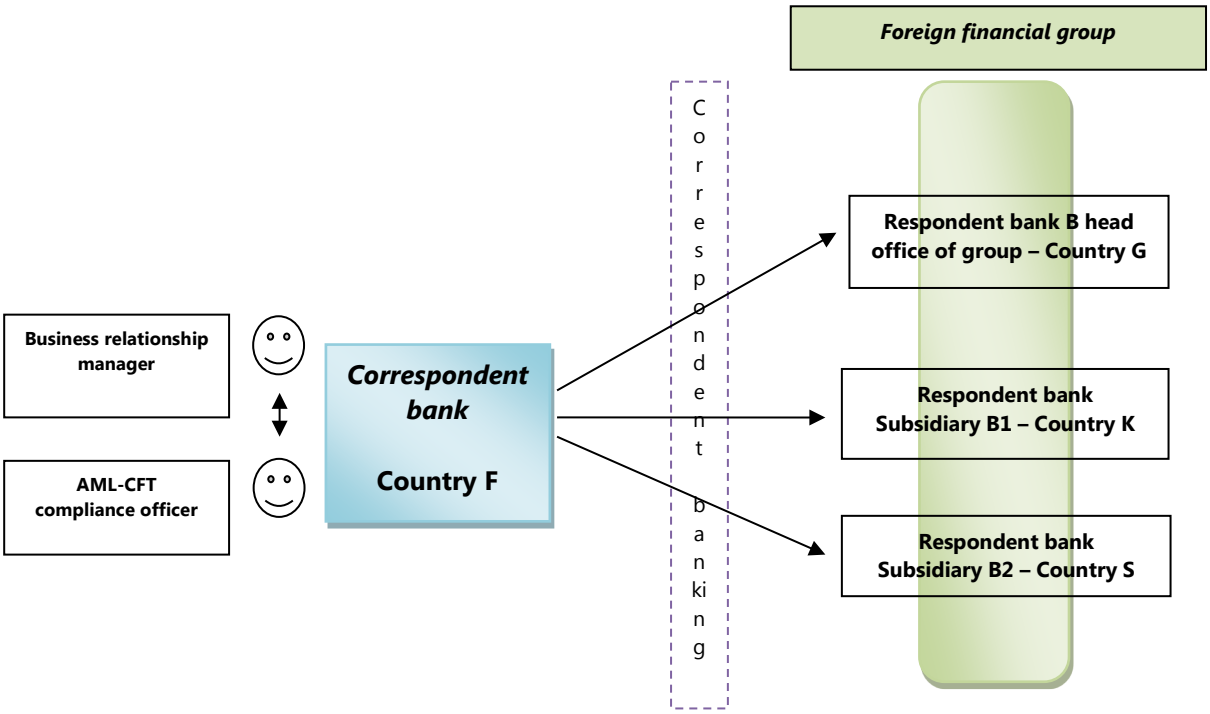
[44] Each entity provides a correspondent banking service in their host country.



Case 1

19. 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 these entities belong to the same group. Nevertheless, the correspondent bank should also assess the ML/FT risks presented by each business relationship.

Case 2



VII. Risk management

20. A bank 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.

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

22. A bank's internal audit and compliance functions[45] 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 and the ongoing monitoring of correspondent banking relationships.

[45] See *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. 40: International cooperation