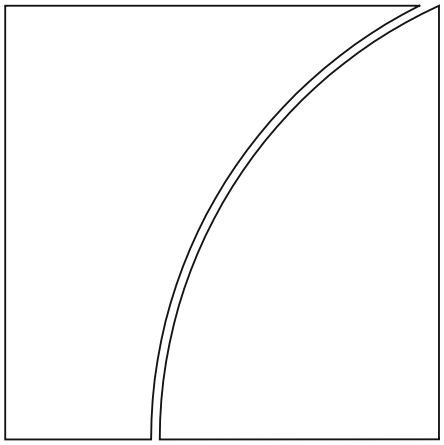
Basel Committee on Banking Supervision

Consultative Document

Guidelines



Revised annex on correspondent banking

Issued for comment by 22 February 2017

November 2016

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9259-009-3 (online)

Contents

Revised annex on correspondent banking

Correspondent banking – revisions to the Basel Committee guidelines on the *Sound management of risks related to money laundering and financing of terrorism*

Background

The text below includes proposed revisions to Annexes 2 ("Correspondent banking") and 4 ("General guide to account opening") of the Basel Committee on Banking Supervision (the Committee) guidelines on the *Sound management of risks related to money laundering and financing of terrorism* first issued in January 2014 and revised in February 2016. The purpose of the proposed revisions is to ensure that banks conduct correspondent banking business with the best possible understanding of the applicable requirements regarding anti-money laundering and countering the financing of terrorism. The clarifications are proposed as the international community has been increasingly concerned about de-risking in correspondent banking, since a decline in the number of correspondent banking relationships may affect the ability to send and receive international payments, or drive some payment flows underground.

The proposed revisions to the Committee's existing guidance follows the publication by the Financial Action Task Force (FATF) of its guidance on *Correspondent banking services*, issued in October 2016. The Committee seeks to clarify concrete regulatory expectations from banking supervisors' point of view consistent with the FATF standards and guidance. In preparing their publications on correspondent banking, the FATF and the Committee worked closely with the FSB, which is coordinating work to assess the extent and address the causes of banks' withdrawal from correspondent banking, through the implementation of a four-point action plan (data collection and analysis, clarifications of regulatory expectations, domestic capacity-building and strengthening the tools for due diligence).

The proposed revisions develop the application of the risk-based approach for correspondent banking relationships, recognising that not all correspondent banking relationships bear the same level of risk. The risk indicators provided should help banks conduct their risk assessment (see in particular paragraphs 7 and 14 in Annex 2). The proposed revisions also clarify supervisors' expectations regarding the quality of payment messages (see added Section VI, paragraphs 31–5) as well as conditions for using "know your customer" (KYC) utilities as recommended in the Committee on Payments and Market Infrastructures (CPMI) report on correspondent banking[1] (see paragraph 18 in Annex 2 and added paragraphs 6bis and 6ter in Annex 4). Annex 4 has not been modified except for these two added paragraphs. Respondents are invited to comment on the content of Annex 2, including on questions raised in boxes, and on proposed paragraphs 6bis and 6ter in Annex 4.

[1] See Committee on Payments and Market Infrastructures, *Correspondent banking*, www.bis.org/cpmi/publ/d147.htm, July 2016.

Annex 2

Correspondent banking

I. General considerations on cross-border correspondent banking

1. According to the FATF glossary, "correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank')". For the purpose of its guidance on correspondent banking (hereafter "the FATF guidance"),[2] the FATF does not include one-off transactions but rather states that correspondent banking is characterised by its ongoing, repetitive nature. Like the FATF guidance, this Annex focuses on higher-risk correspondent banking relationships, especially cross-border correspondent banking.

2. Used by banks throughout the world, correspondent banking services enable respondent banks to conduct business and provide services[3] that they cannot offer otherwise (owing to the lack of an international presence and cross-border payment systems). As mentioned by the Financial Stability Board, the ability to make and receive international payments via correspondent banking is vital for businesses and individuals, and for the G20's goal of strong, sustainable, balanced growth.[4]

3. Correspondent banks execute and/or process transactions for customers of respondent banks. Correspondent banks generally do not have direct business relationships with these customers, which may be individuals, corporations or financial services firms, established in jurisdictions other than that of the correspondent bank. Thus the customers of the correspondent bank are the respondent banks.

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

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

5. The FATF guidance clarifies that, while correspondent banking in general is considered higher-risk, not all correspondent banking services carry the same level of ML/FT risks. The FATF guidance focuses on cross-border correspondent banking relationships involving the execution of third-party payments that are higher-risk.[5] This section provides factors that banks should take into account when assessing the level of risk of a particular correspondent banking relationship.

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

3 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".

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

5 See FATF, *Guidance on correspondent banking services*, October 2016, paragraph 13a.

A. Risk indicators and risk assessment

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

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

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

- (a) the purpose of the services provided to the respondent bank (eg foreign exchange services for respondents' proprietary trading, securities trading on recognised exchanges or payments between a respondent's group within the same jurisdiction may constitute indicators of lower risk);
- (b) whether different entities of the group to which the respondent bank belongs would have access to the account;
- (c) the ability of other third parties to have access to the correspondent account, such as payable through accounts or "nested" relationships (see paragraph 10 below).

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

- (d) the respondent bank's major business activities including target markets and overall types of customers served in key business lines;[6]
- (e) the respondent bank's management and ownership (including the beneficial owners) and whether they represent specific ML/FT risks (eg politically exposed persons (PEPs));
- (f) the respondent bank's money laundering prevention and detection policies and procedures, including a description of the customer due diligence (CDD) measures applied by the respondent bank to its customers and the correspondent bank's ability to obtain information on a particular transaction as specified in paragraphs 32–3 of the FATF guidance;[7]
- (g) whether any civil, administrative or criminal actions or sanctions, including public reprimands, have been applied by any court or supervisory authority to the respondent bank.

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

- (h) the jurisdiction in which the respondent bank (and its parent company when the respondent bank is an affiliate) is located;
- (i) the jurisdictions in which subsidiaries and branches of the group may be located, possibly using the group structure available in the Legal Entity Identifier (LEI) system,[8]

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

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

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

as well as the jurisdictions in which third parties having access to the correspondent account may be located;

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

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

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

B. Nested (downstream) correspondent banking

10. 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.

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

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

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

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

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

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

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

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

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

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

15. Correspondent banks should ensure respondent banks promptly respond to requests for information (see FATF guidance, paragraph 32) related to transactions through respondent banks, as appropriate.

C. Information-gathering

16. Before entering into a business relationship with a respondent bank, correspondent banks should gather sufficient information to fully understand the nature of the respondent's business and assess ML/FT risks both at the outset and on an ongoing basis. There is no requirement or expectation for a correspondent bank to apply CDD measures to customers of the respondent bank or to duplicate the data on its customers obtained and stored by the respondent bank.

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

18. At account opening, banks may collect – and subsequently update – respondent bank information by using third-party databases that contain relevant information on banks (often referred to as "KYC utilities"). KYC utilities may provide efficiency gains for both correspondent and respondent bank to gather and provide information. From the correspondent bank perspective, using a KYC utility could in particular be useful for gathering information on the respondent bank, especially to assess the factors listed in paragraph 7. The conditions and factors to consider when using KYC utilities under the final responsibility of the correspondent bank are described in paragraph 6bis and 6ter of Annex 4.

Box 1

Information from KYC utilities on respondent banks' overall customer base or types of customers

Q. Would it be useful for this guidance to further detail the sort of information a correspondent bank could acquire from a KYC utility on the respondent's customer base? Do you agree that the information set out below could be useful and realistically obtained?

There is no requirement to perform CDD on a respondent bank's individual customers. However, correspondent banks may find it useful to gather information on respondent banks' profiles through KYC utilities. Useful information on respondent bank customer types could include: (i) a broad classification according to economic sectors such as the System of National Accounts classification, distinguishing between corporations (using their accounts to support their economic activity of producing goods or services or accumulating capital), households, government, non-profit institutions, and other factors such as the distinction between financial and non-financial corporations and the size of the corporation or of the corporate group to which the corporation belongs; (ii) the proportion of resident and non-resident

customers and countries of the non-resident customers; and (iii) whether certain high-risk categories (such as PEPs) are over-represented in the customer base compared to the general population. To the extent improvements in the content of payment messages allow this, such as with the inclusion of ISO country codes and the LEI, some of this information can be obtained and updated through the analysis of the flow of messages of the respondent bank, as this will provide information on the customers using correspondent banking services.

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

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

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

21. All correspondent banking relationships should be subject to an appropriate level of due diligence following a risk-based approach, as presented above. The level of due diligence should be proportionate to the respondent bank's risk profile and consistent with paragraph 14 of the FATF guidance. Banks should not treat the CDD process as a "paper-gathering exercise" but as an essential step to support assessment of ML/FT risk, as described in paragraphs 7–9. This involves the correspondent bank assessing the respondent bank's AML/CFT controls on a risk-sensitive basis (for example, receiving a description of the respondent bank's AML/CFT procedures and systems, including sanctions screening, checking if the internal audit function regularly reviews the adequacy of the respondent bank's AML/CFT controls) consistent with the FATF guidance and the main body of the present guidelines. Where appropriate, the information-gathering should be complemented by liaising directly (eg by phone or videoconference) with the respondent bank's local management and compliance officer, or potentially by an on-site visit.

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

Box 2

Assessment of a respondent bank's AML/CFT programme

Q. Would it be useful for the Committee to elaborate further on how a correspondent bank should conduct the assessment of a respondent bank's AML/CFT policies and procedures, eg via the use of internal audit reports, or are paragraphs 21–2 sufficient in that respect?

IV. Customer acceptance and retention

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

24. Pursuant to the FATF standards (Recommendation 13), correspondent banks should refuse to enter into or continue correspondent banking relationships with "shell" banks (ie banks incorporated in a jurisdiction in which they have no physical presence and which is unaffiliated with a regulated financial group).[9] Correspondent banks should not enter into correspondent banking relationships if they are not satisfied, based on the information gathered or received, that the respondent bank is not a shell bank.

V. Ongoing monitoring

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

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

27. If a correspondent bank decides to allow correspondent accounts to 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 the specific risks assessed. The correspondent bank should verify that the respondent bank has conducted adequate CDD on the customers with direct access to correspondent accounts and that the respondent bank can provide relevant CDD information upon request.

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

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

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

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

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

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

32. In particular, the quality of information provided in payment messages should be part of the ongoing monitoring. Indeed, as mentioned in the Committee guidance on payment messages,[10] the correspondent bank should monitor the payment messages transmitted by the respondent bank for the purpose of detecting those which lack required originator and/or beneficiary information consistent with straight through processing, and verify the reliability of the respondent's controls, for instance via sample testing (ie a closer look at a few transactions to identify cases where they do not comply with the wire transfer information requirements).

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

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

35. As stated in paragraph 31, intermediary banks should monitor payment messages for manifestly meaningless or incomplete fields. As recommended by the CPMI, the use of the LEI as additional information in payment messages should be possible on an optional basis in the current relevant payment messages (ie MT 202 COV and MT 103). Where available, the use of the LEI would facilitate the determination by the correspondent bank that the information in the message is sufficient to unambiguously identify the originator and beneficiary of a transfer.

Box 3

Quality of payment messages

The paragraphs above are mainly based on the Committee publication *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*. This publication also sets out the role of supervisors in checking the banks' implementation of due diligence regarding payment messages (see paragraphs 37–40 of that publication, www.bis.org/publ/bcbs154.pdf). The Committee guidelines *Sound management of risks related to money laundering and financing of terrorism* to which the present Annex is appended also develop the role of supervisors (see paragraphs 84–95). Both documents are relevant in the context of this Annex on correspondent banking.

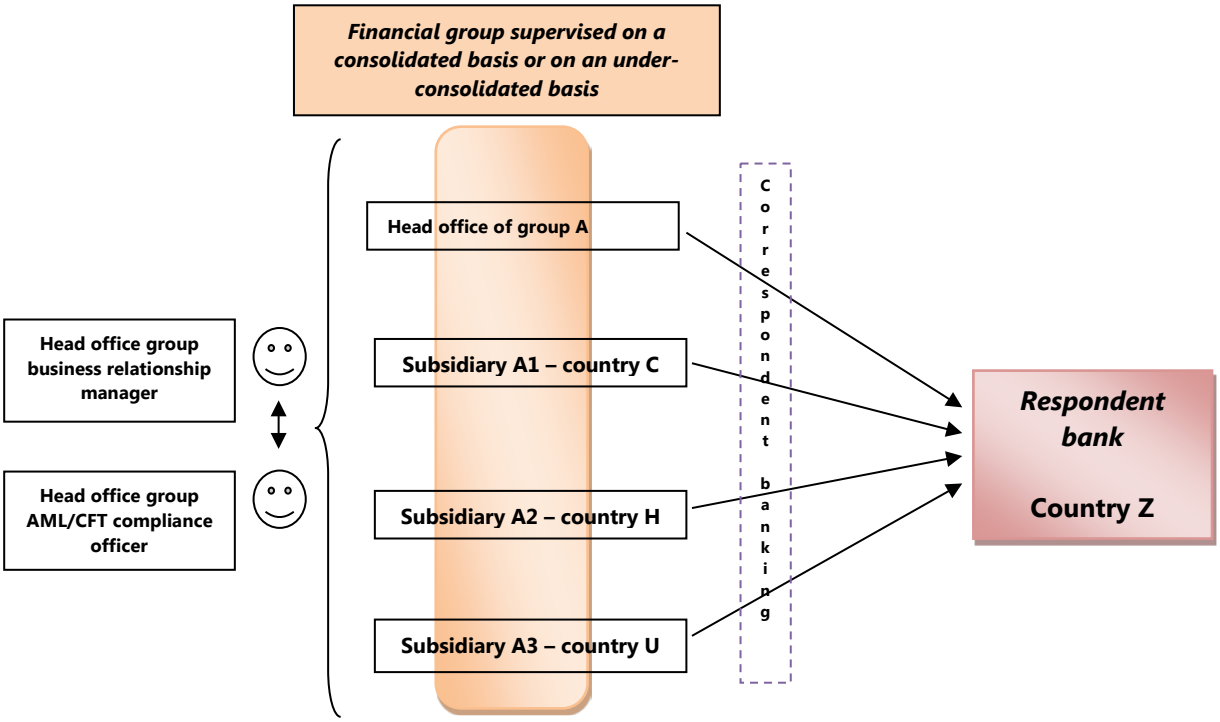
Q. Considering the existing Committee publication, would it be useful to: (i) insert the content already included in paragraphs 37–40 of the 2009 publication in this Annex, or (ii) detail further the expectations with respect to quality of payment messages, and, if yes, do you have suggestions?

[10] See in particular paragraph 31 of Basel Committee on Banking Supervision, *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, May 2009.

VII. Group-wide and cross-border considerations

35. If a respondent bank has correspondent banking relationships with several entities belonging to the same group[11] (case 1), the head office of the group should ensure that the assessments of the risks by the different entities of the group are consistent with the group-wide risk assessment policy. The group's head office should coordinate the monitoring of the relationship with the respondent bank, particularly in the case of a high-risk relationship, and make sure that adequate information-sharing mechanisms inside the group are in place.

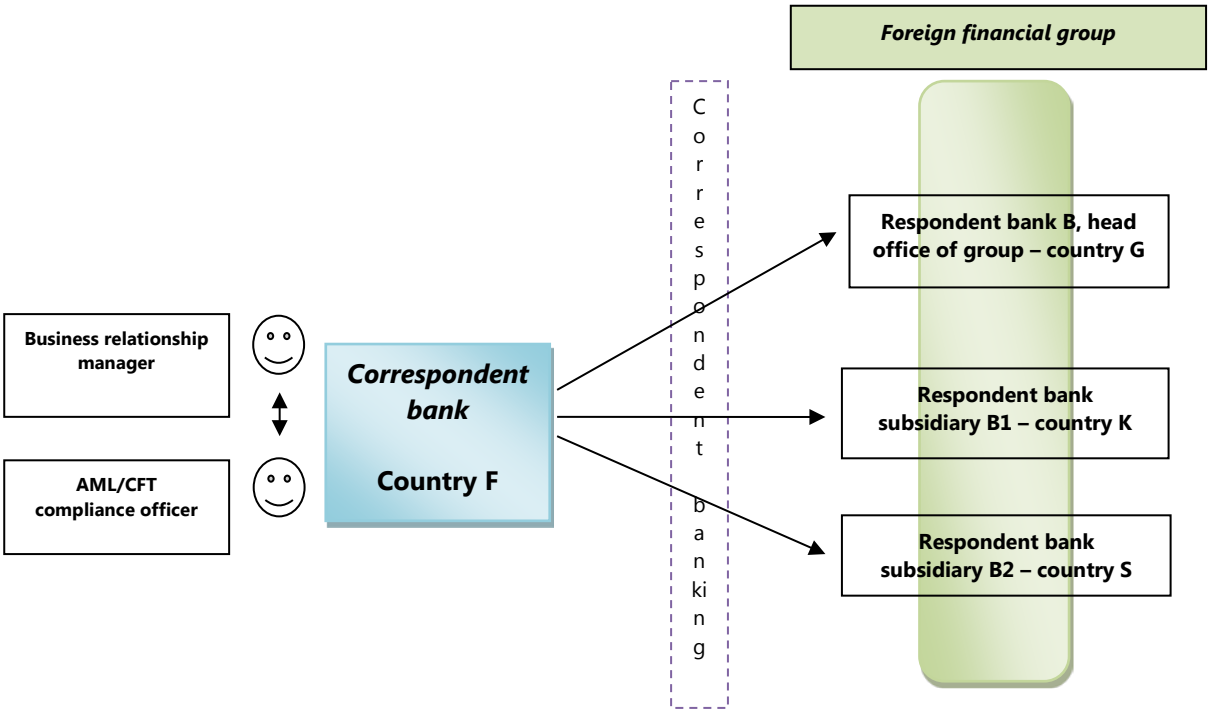
Case 1



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

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

Case 2



VIII. Risk management

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

38. Including notice periods for terminating or limiting the business relationships in the terms and conditions governing the correspondent banking relationship is recommended as it should be part of the correspondent bank's risk management procedures. From the respondent bank's perspective, such notice periods should inform banks' business continuity plans.[12] As part of contingency planning for critical functions under operational risk management, a respondent bank may consider having more than one correspondent banking account for its payment services, where necessary for its continued operation.

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

39. A bank's internal audit and compliance functions[13] have important responsibilities in evaluating and ensuring compliance with procedures related to correspondent banking activities. Internal controls should cover identification measures of the respondent banks, the collection of information, the ML/FT risk assessment process, ongoing monitoring of correspondent banking relationships and compliance with the duties to detect and report suspicions (about respondents and/or possible underlying subjects involved in the transactions).

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

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

Annex 4

Disclaimer for public consultation: The final version of the General guide to account opening was issued in February 2016 and has not been reviewed in its entirety. Rather, the present consultation only concerns the added paragraphs 6bis and 6ter (in bold characters).

General guide to account opening

I. Introduction

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

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

3. The guidance set out in this annex is therefore intended to assist banks in defining their approach to account opening. It may be adapted for specific application by banks in respect of their AML/CFT policies and procedures, especially in developing sound customer risk profiles and by national financial supervisors seeking to further enhance the effectiveness of bank compliance with customer identification and verification programmes. Supervisors recognise that any effective customer identification/verification programme should reflect the risks arising from the different types of customer, types of banking product and the varying levels of risk resulting from a customer's relationship with a bank. Higher-risk customer relationships and transactions, such as those associated with PEPs[14] or other higher-risk customers, will clearly require greater scrutiny than relationships and transactions associated with lower-risk customers. Therefore, the provisions in this guide should be read in conjunction with the main body of the guidelines, and in particular with the provisions related to assessing and understanding risks (see paragraphs 15–16 of the guidelines) and should be adapted for identified specific (higher- or lower-) risk situations.

4. Guidance and best practice established by national financial supervisors should be commensurate with the risks present in the jurisdiction; for this reason they will vary between countries. According to this risk-based approach, jurisdictions may allow simplified customer due diligence measures to be applied for lower-risk situations. For example, some jurisdictions have either taken or supported actions to encourage financial inclusion by promoting lower-risk financial products (such as an account

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

with a limited set of services for specific types of customer). Conversely, in cases where there is a higher risk, banks should apply enhanced due diligence. Examples of such cases include the customer applying for specific products featuring non-face-to-face transactions, that allow anonymity of certain transactions,[15] or that are specifically vulnerable to fraud.

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

6. According to the FATF standards,[16] banks should always identify customers and verify their identity.[17] When doing so, banks should be conscious that some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the validity of the document(s) presented, the verification requirement should be enhanced and the information provided by the customer should be verified through additional inquiries or other sources of information.

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

(a) helping identify the customer, by providing identification information;

(b) collecting information supporting the risk profile;

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

Such utilities may be used at different stages, for instance at account opening for obtaining basic information, during the course of the relationship to update the information, or on an ongoing basis to assist banks with gathering information for their risk assessment process. Banks should take into account international standards, which require consideration of the reliability of the source,[18] and compliance with applicable national laws, which may prescribe certain customer identification or verification procedures. Banks should also be alert to the risk of identity theft, and take into account the fact that a database may help establish that a customer exists and gather information on that customer. However, the database may not necessarily confirm that the person the bank is dealing with is that customer.

6ter. In any case, the ultimate responsibility for CDD remains with the bank. The level of risk associated with the customer and the KYC utility features will determine whether the bank needs to verify or corroborate the information provided by the utility and collect additional information,

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

[16] See FATF Recommendation 10.

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

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

or take other measures. Therefore, when determining the extent to which they can use KYC utilities to support due diligence, banks should consider whether:

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

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

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

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

II. Natural persons

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

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

Natural persons

Identification information

Table 1

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

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

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

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

B. Information related to the customer's risk profile

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

Natural persons

Risk profile's information

Table 2

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

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

C. Verification of identity of natural persons

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

(a) Documentary verification procedures[19]

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

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

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

(b) Non-documentary verification procedures

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

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

D. Further verification of information on the basis of risks

12. Particular attention needs to be focused on those customers assessed as having higher-risk profiles.[20] Additional sources of information and enhanced verification procedures may include:

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

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

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

III. Legal persons and arrangements and beneficial ownership

15. The procedures discussed previously in paragraphs 8–14 should also be applied to legal persons and arrangements. Banks should identify and verify the identity of the customer, and understand the

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

nature of its business, and its ownership and control structure, with a view to establishing a customer risk profile.

A. Legal persons[21]

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

1. Identification of legal persons

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

Legal persons

Identification information

Table 3

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

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

(b) The term "beneficial owner" is used in this annex in a manner consistent with the definition and clarifications provided in the FATF standards. For reference, the FATF defines a "beneficial owner" as the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

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

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

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

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

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

Legal persons

Risk profile information

Table 4

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

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

3. Verification of identity of legal persons

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

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

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

(a) Documentary verification

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

(b) Non-documentary verification

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

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

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

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

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

5. Further verification of information on the basis of risks

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

B. Legal arrangements[22]

1. Identification of legal arrangements

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

Legal arrangements

Identification information

Table 5

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

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

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

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

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

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

Legal arrangements

Risk profile information

Table 6

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

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

3. Verification of identity of legal arrangement

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

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

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

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

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

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

5. Further verification of information on the basis of risks

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

C. Focus on specific types of customer

1. Retirement benefit programmes

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

2. Mutuals/friendly societies, cooperatives and provident societies

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

3. Professional intermediaries

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

34. Where such circumstances apply and an account is opened for an open or closed-end investment company, unit trust or limited partnership that is subject to customer due diligence requirements which are equivalent to those applying to the bank itself, the bank should treat this investment vehicle as its customer and take steps to identify:[23]

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

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

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

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