

—
P O Box 427 Pretoria 0001 South Africa
370 Helen Joseph Street Pretoria 0002
+27 12 313 3911 / 0861 12 7272
www.resbank.co.za



Ref.: 15/8/2

G5/2022

To: All banks, controlling companies, branches of foreign institutions, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Supervisory guidelines for matters related to the prevention of banks or controlling companies being used for any money laundering or other unlawful activity

Executive summary

The purpose of this guidance note is to inform and bring to the attention of banks and controlling companies practices related to effective implementation of adequate anti-money laundering and combating terrorist financing (AML/CFT) group controls in the operation of their respective group entities.

Regulation 39, 36(17) and 50 of the Regulations relating to Banks (Regulations) require every bank and every controlling company, among others, to have in place board approved policies and comprehensive risk-management processes and procedures, which policies, processes and procedures include comprehensive and robust know-your-customer standards that inter alia include robust customer identification, verification and acceptance requirements throughout the banking group, contribute to the safety and soundness of the reporting bank or controlling company, and prevent the bank or controlling company or other relevant entities within the group from being used for any money laundering or other unlawful activity.

Furthermore, regulation 36(17) of the Regulations requires, among others, that the aforementioned policies, processes and procedures must be sufficiently robust and ensure that the bank or controlling company inter alia continuously receives relevant information relating to risk exposure incurred by any foreign operation and that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies AML/CFT measures consistent with the relevant Financial Action Task Force (FATF) Recommendations issued from time to time; the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.

1. Introduction

- 1.1. Recommendation 18 of the FATF Recommendations¹ specifically mentions that:

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

- 1.2. Requirements for preventive measures are dealt with in the Financial Intelligence Centre Act 28 of 2001 (FIC Act) which requires the application of a risk-based approach when dealing with matters of customer due diligence.
- 1.3. The Basel Committee on Banking Supervision Guidelines (BCBS guidelines) on the sound management of risks relating to ML/FT² emphasises that consolidated risk management means establishing and administering a process to coordinate and apply policies and procedures on a group-wide basis across its international operations.
- 1.4. This guidance note therefore serves to inform and assist banks with more information concerning the effective implementation of group controls.
- 1.5. Regulation 38(4) of the Regulations states, among others, when the Authority is of the opinion that a bank's policies, processes and procedures relating to its risk assessment or internal control systems are inadequate, the Authority may require the bank, among others-
- (i) to strengthen the bank's risk management policies, processes or procedures; or
 - (ii) to strengthen the bank's internal control systems.

2. The implementation of AML/CFT group controls in banks' and controlling companies' foreign operations

- 2.1. In terms of the Form BA 099A completed by foreign operations in terms of the Regulations, banks under section B are required to declare that they comply with the local AML/CFT legislation within their region.

¹ <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

² <https://www.bis.org/bcbs/publ/d505.pdf>

- 2.2. Regulation 36(17) of the Regulations specifically requires that every relevant foreign branch, subsidiary or operation of the bank or controlling company apply AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time; the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.
- 2.3. Where such home country AML/CFT standards cannot be implemented in a host country, the Chief Executive Officer of the relevant bank or controlling company has to inform the Prudential Authority (PA) accordingly, in writing.
- 2.4. BCBS guidelines highlight that group policies and procedures should be designed to also identify, monitor and mitigate group-wide risks in addition to compliance with relevant laws and regulations.
- 2.5. Section 42(2)(q) of the FIC Act specifically requires that a bank's risk management and compliance programme (RMCP) provides for the manner in which the RMCP is implemented in branches, subsidiaries or other operations of the institution in foreign countries.
- 2.6. The aforementioned will enable the institution to comply with its obligations in terms of the FIC Act, and requires the institution to determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under the FIC Act.
- 2.7. The bank must inform the Financial Intelligence Centre (FIC) and the PA in writing if the host country does not permit the implementation of measures required under the FIC Act³.
- 2.8. Banks are required to effectively implement adequate AML/CFT group controls in the operations of their foreign entities, and financial institutions themselves must report that they apply the stricter AML/CFT standards in home-host situations, often but not exclusively applying the South African requirements through setting up group-wide AML/CFT programmes and standards.
- 2.9. It is essential that the group AML/CFT function has a structured approach to ensuring that group-wide AML/CFT programmes and standards are regularly communicated to foreign subsidiaries, and that the foreign subsidiary/branch is updated in terms of any changes thereto.
- 2.10. The PA acknowledges that many large banking groups with the capability to do so centralise certain processing systems and databases for more effective management and to create efficiencies. When implementing this, adequate documentation of such functions is required, such that the local and centralised transaction/account monitoring functions ensure that the opportunity to monitor for patterns of potential suspicious activity across the group and not just at either the local or centralised level⁴.

³ Section 42(2)(q)(iii) of the FIC Act

⁴ Para 74 of the BCBS Guidelines- Sound Management of risk related to money laundering and financing of

2.11. The group-wide AML/CFT programmes and standards must be effectively implemented, be consistent and cover a broad range of topics relating to group standards and policies, e.g. customer due diligence requirements, enhanced due diligence requirements, the identification of domestic and foreign public prominent officials, sanctions screening requirements, due diligence measures linked to trade finance clients, the requirements for ongoing and enhanced monitoring for higher risk clients etc.

3. Ensuring effective implementation of group controls

3.1. Effective implementation of group controls across the group requires that there are sufficient and adequate skills and resources able to assist with the implementation of group solutions in a timely manner.

3.2. Additionally, assurance as to the effectiveness of implementation can be provided through the group audit and compliance functions, including initiatives such as ongoing training and assurance testing as part of the RMCP. External third parties with the appropriate skills set of technical AML/CFT knowledge may also provide assurance to banks or controlling companies in terms of the effectiveness of the implementation of group controls designed to mitigate and manage ML/TF risk posed to the bank or controlling company. Such overall group functions need to be strong as they are primary mechanisms for monitoring the overall application of the bank or controlling company's global customer due diligence and the effectiveness of its policies and procedures and controls⁵.

3.3. Group audit (internal or external) plays a key role in assessing the effectiveness of controls and the group audit plan devised must reflect a scope and frequency of audit of the groups' AML/CFT based on risk.

3.4. A group/chief AML/CFT officer for group wide compliance with all relevant AML/CFT policies, procedures and controls nationally and abroad is important for effective group wide risk mitigation.

3.5. The group AML/CFT oversight function in respect of the AML/CFT operations and controls in foreign subsidiaries or other relevant operations, must have access to adequate and reliable pertinent risk data held by the host country to enable it to check and challenge the application of group AML/CFT standards, policies, procedures within the foreign subsidiary or branch⁶.

terrorism

⁵ Para 68 of the BCBS Guidelines- Sound Management of risk related to money laundering and financing of terrorism

⁶ Section 4 of the interpretive note to recommendation 18 : Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management

- 3.6. To enable effective group wide monitoring, banks and controlling companies should thus be authorised to share information about their customers, subject to adequate legal protection, with their head offices or parent bank⁷.
- 3.7. Within South Africa, in terms of section 37 of the FIC Act, no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by an accountable institution (bank) or supervisory body as it relates to:
- (i) reporting duties and access to information;
 - (ii) measures to promote compliance by accountable institutions; and
 - (iii) compliance and enforcement.
- 3.8. In South Africa, section 38 of the Protection of Personal Information Act 4 of 2013 (POPIA) provides for an exemption in respect of certain functions, in particular, any function conferred on any person in terms of the law, which is performed with the view to protect members of the public against:
- (i) Financial loss due to dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or
 - (ii) Dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity.
- 3.9. The protection of personal information as provided for in the POPIA is applicable to the FIC and the PA, as per the aforementioned and must be interpreted in a manner as prescribed in section 3 of the POPIA.
- 3.10. Pertinent foreign law may enable similar provisions regarding the disclosure of personal information and should be considered by host and home countries.
- 3.11. Where host countries are employing legislation that is more onerous than that contained in the home country's framework, the host country must communicate this to the group AML/CFT function.
- 3.12. In relevant cases, when a home country bank responsible for oversight of AML/CFT has conducted a review of the host country's AML/CFT legislative regime against the AML/CFT requirements of the home country, and the group AML/CFT requirement cannot be implemented or effected by a host country, the bank must provide the PA and the FIC with a written notification from the host country's responsible supervisor of the relevant information and circumstances.

⁷ Para 66 of the BCBS Guidelines- Sound Management of risk related to money laundering and financing of terrorism

- 3.13. Home country bank employees will benefit from regular and robust engagement with host country bank employees charged with AML/CFT functions and having in place regular reporting mechanisms whereby the home country may be placed in a position to adequately assess the ML/TF control measures implemented as well as adherence to group ML/TF standards and requirements.
- 3.14. Adequate procedures to inform necessary stakeholders and home banks of any risk events occurring at a host bank which threaten sound management and mitigation of ML/TF risk should be implemented, as well as appropriate mechanisms for resolution thereof as soon as possible.
- 3.15. Effective and ongoing training of staff at host and home country banks is an effective tool for ensuring effective implementation of group controls.
- 3.16. When assessing a bank or controlling company's compliance with group-wide AML/CFT policies and procedures as well as the assessment of the effectiveness of group-wide controls during on-site inspections home country supervisors should not face impediments.
- 3.17. On-site visits to host jurisdictions by home country banks and home country supervisors assist in ensuring that there are effective group controls in place and host foreign banks should provide an appropriate legal framework to facilitate the passage of information required for risk management purposes to the head office or parent bank and the PA.

4. Terminology

4.1.

Term	Definition
Recommendation 18	Refers to the Financial Action Task Force Recommendation 18 of the Forty Recommendations
Customer due diligence	Measures undertaken to mitigate ML/TF risk associated with a proposed business relationship or single transaction.
Enhanced due diligence	Circumstances where the risk of money laundering or terrorist financing is higher and enhanced due diligence measures need to be undertaken. Those measures applied which seek to be effective and proportionate to address an elevated degree of ML/TF risk.

5. Acknowledgement of receipt

- 5.1 Kindly ensure that a copy of this guidance note is made available to your institution's independent auditors. The attached acknowledgement of receipt, duly completed and signed by both the Chief Executive Officer of the institution and the said auditors, should be returned to the PA at the earliest convenience of the aforementioned signatories.

Fundi Tshazibana
Chief Executive Officer

Date:

The previous guidance note issued was Banks Act Guidance note 4/2022, dated 09 May 2022.