


 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

G6/2022

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 the formulation of appropriate business risk assessments which contribute to effective money laundering and terrorist financing (ML/TF) and proliferation financing (PF) risk management.

Section 64A of the Banks Act, 1990 read with regulation 39, 50 and 36(17) of the Regulations relating to Banks (Regulations) requires that every bank and every controlling company shall 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 any other relevant entity in 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 anti-money laundering and combating terrorist financing (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. The FATF Guidance on the risk-based approach in the banking sector¹ clearly stipulates that the risk assessment forms the basis of a bank's risk-based approach. It must enable the bank to understand how, and to what extent, it is vulnerable to ML/TF/PF. It necessitates an evidence-based and informed categorisation of risk at various levels, which will help banks determine the level of AML/CFT or counter-proliferation financing (CPF) resources necessary to mitigate that risk. All relevant information must always be properly documented, maintained and communicated to relevant personnel within the bank, controlling company and other relevant group entities.
- 1.2. The requirements for preventive measures are dealt with in the Financial Intelligence Centre Act 28 of 2001 (FIC Act) and requires the application of a risk-based approach when dealing with matters concerning customer due diligence.
- 1.3. The PA acknowledges that in the context of banks, holding companies, controlling companies and/ or banking groups, detailed and thorough business risk assessments are imperative for the demonstration of thorough ML/TF/PF risk appreciation specific to all relevant group entities.
- 1.4. Two critical steps for the ML/TF/PF business risk assessment (business risk assessment) are the following:
 - 1.4.1. identification of ML/TF/PF risk; and
 - 1.4.2. assessment of ML/TF/PF risk.
- 1.5. Effective and sound business risk identification and assessments enable banks and controlling companies to implement the most adequate and appropriate risk monitoring, mitigating and management controls.
- 1.6. The business risk assessment must be conducted systematically while including a sufficient range of inherent risk factors to identify and reflect an in depth understanding of ML/TF/PF risk at an institutional level.
- 1.7. 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-
 - 1.7.1. to strengthen the bank's risk management policies, processes or procedures;
or
 - 1.7.2. to strengthen the bank's internal control systems.

¹ <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

2. Identification of ML/TF/PF risk

- 2.1. The identification of ML/TF/PF risk requires banks and controlling companies to consider appropriate and pertinent data from various sources, for example; national risk assessments in line with FATF Recommendation 1.
- 2.2. Banks and controlling companies must consider the national legal and regulatory framework, including any areas of prescribed significant risk and any mitigation measures defined at legal or regulatory level². Data from sector risk assessments may also be considered.
- 2.3. Other local and foreign data sources may also include the following³:
 - 2.3.1. law enforcement alerts and reports;
 - 2.3.2. thematic reviews and similar publications issued by competent authorities;
 - 2.3.3. government policy statements and alerts;
 - 2.3.4. explanatory memorandums to relevant legislation;
 - 2.3.5. information from regulators, such as guidance and the reasoning set out in regulatory fines;
 - 2.3.6. information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies;
 - 2.3.7. information obtained as part of the initial customer due diligence process and ongoing monitoring;
 - 2.3.8. credible information from industry bodies, such as typologies and emerging risks;
 - 2.3.9. information from civil society, such as corruption indices and country reports;
 - 2.3.10. information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists; and
 - 2.3.11. information from credible and reliable commercial organisations, such as risk and intelligence reports; and
 - 2.3.12. information from statistical organisations and academia.

3. Assessing ML/TF/PF risk

- 3.1. Banks and controlling companies must determine how the ML/TF/PF threats identified will affect them. This determination can be achieved when sufficient information is obtained to understand the likelihood of these risks occurring, and the impact that these would have on the individual banks, controlling companies, the banking sector and possibly on the national economy for large scale, as well as systemic financial institutions, if they did occur⁴.
- 3.2. Consideration of respective threats and vulnerabilities against the business of the bank and other relevant group entities is thus necessary. For example, a bank with a high volume of domestic prominent influential persons (PIPs) should consider how corruption risk linked to domestic PIPs impacts it, even more so where this has already been recognised as a national risk within a specific jurisdiction of operation.

² Para 18: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

³https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

⁴ Para 22: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

- 3.3. As such, it is also prudent to always give regard to the aforementioned factors in the context of risk. This includes considering the risk profile of the country within which the bank, controlling company or foreign branches and subsidiaries conduct business, for example corruption risk in the context of a bank that mostly banks politically exposed customers as clients with strong ties to state owned entities and private companies. Such considerations enhance a bank or controlling company's appreciation for its own vulnerability to abuse by such client types.
- 3.4. The ML/TF/PF risks a bank or group is exposed to differs from bank to bank and it is possible that one bank could have a higher level of ML/TF/PF risk to manage given its risk profile than another.
- 3.5. The degree of exposure to ML/TF/PF risk must be informed by each business area of a bank, controlling company and their relevant foreign operations, which may present differing degrees of ML/TF/PF risks and are often dependent on consideration of the factors such as client risk, geographical risk, products and services, delivery channels, transactional risk etc. Data collection is thus essential for the understanding and assessment of ML/TF/PF risk.

All relevant clients of entities within the group could be classified as high, medium or low risk from a ML/TF/PF perspective and some may emanate from high-risk sectors and industries for example: arms manufacturers, dealers in precious stones and metals, cash intensive businesses and numerous unregistered non-profit organisations with a presence in high-risk jurisdictions. These client type considerations influence the ML/TF/PF risk profile of a bank at an institutional level.
- 3.6. For subsidiaries, ML/TF/PF business risk assessments are effective when conducted in the context of the ML/TF/PF risk presented in the country, weighed against consideration of factors such as its own clients, products, financial flows, delivery channels etc.
- 3.7. Correspondent banking (CB) relationships may also have an impact on a bank's ML/TF/PF risk profile, i.e. some banks may have far fewer correspondent banking relationships and others may have multiple CB relationships acting as correspondents to banks that have weak AML/CFT programmes.
- 3.8. Banks are deposit taking institutions, and in some instances other entities may partner with a bank to offer certain money or value transfer services. These relationships held by banks with such entities presents potential additional ML/TF/PF risk to a bank and must thus also form part of the business risk assessment consideration.
- 3.9. Taking into account the transactional data a bank, holding company, controlling company and/or banking group has access to, it is useful to reflect the understanding of inflows and outflows in the business risk assessment to the extent that the transactional flows and the risk associated therewith is understood. For example, a bank may be aware of high volumes of outflows of funds to specific high-risk jurisdictions in respect of high-risk clients.

- 3.10. Consideration of the use of cash and the ML/TF/PF risk associated with cash in the context of a bank's business is also important. For example, when frequent cash deposits are made by non-clients with little due diligence being performed to mitigate the risk associated with such funds.
- 3.11. Banks and controlling companies must give regard to the trends and emerging ML/TF/PF risks which can be considered for inclusion in the business risk assessment.
- 3.12. As such, banks and controlling companies must ensure that they have processes, systems and controls in place to identify emerging ML/TF/PF risks and that they can assess these risks and, where appropriate, incorporate them into their risk assessments in a timely manner.
- 3.13. Data feeding into the risk assessment must be regularly tested and validated for integrity, accuracy, and quality.
- 3.14. Prior to new products being introduced, these must be assessed from a ML/TF/PF risk perspective, and this must be reflected in the business risk assessment.
- 3.15. As ML/TF/PF risk is ever changing, banks and controlling companies are required to be agile, forward looking and dynamic in their approach to their assessment and consideration of ML/TF/PF risk, and this must be reflected through regular periodic reviews and updates thereto. Trigger events may warrant updates to the business risk assessment outside of normal and expected timeframes within a bank.
- 3.16. The aforementioned details are not exhaustive and any other relevant information must be considered by the bank and controlling company when conducting their respective institutional risk assessments.
- 3.17. Banks and controlling companies must have appropriately skilled and trusted employees who are technically equipped to perform the task of the business risk assessment, which must be commensurate with the complexity of the bank or controlling company's operations⁵.

4. Trigger Events

- 4.1. A trigger event is an instance which is indicative that the bank or controlling company must review its risk assessment and in turn the controls and how they impact the broader AML/CFT/CPF) programme.
- 4.2. Examples of trigger events may include the following⁶:
 - 4.2.1. There is a noticeable change in customer uptake or use of a product or channel;
 - 4.2.2. There is a noticeable change/uptake in the volume or value of relevant transactions;

⁵ Para 23: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

⁶ <https://www.austrac.gov.au/sites/default/files/2020-08/AUSTRAC%20Insights%20-%20Assessing%20ML-TF%20Risk.pdf>

- 4.2.3. the bank makes a change to a product or channel, and additional features are thereafter applicable to the channel or product;
- 4.2.4. the transaction monitoring identifies unusual patterns of activity;
- 4.2.5. the ongoing customer due diligence identifies unusual patterns of activity;
- 4.2.6. the financial crime compliance function identifies threats or emerging trends of criminal exploitation of a product or channel;
- 4.2.7. a change in the external environment leads to a change in the bank or controlling company's exposure to risk, and
- 4.2.8. the financial intelligence unit or law enforcement communicates information about the ML/TF/PF risks of a product or channel within the bank.

5. Risk factor consideration examples⁷

5.1. For purposes of undertaking a business risk assessment, examples of risk factor considerations that may be relevant are listed below.

5.1.1. Client risk

- 5.1.1.1. The customer and the customer's beneficial owner's business or professional activity.
- 5.1.1.2. The customer and the customer's beneficial owner's reputation; and the customer's and the customer's beneficial owner's nature and behaviour.
- 5.1.1.3. Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
- 5.1.1.4. Where the customer is a legal person, trust, or other type of legal arrangement, what is the purpose of their establishment and what is the nature of their business?
- 5.1.1.5. Do the customers have political connections, for example, are they a domestic prominent influential person (DPIP) or a foreign prominent public official (FPPO) or is their beneficial owner a DPIP/FPPO? Does the customer or beneficial owner have any other relevant links to a DPIP/FPPO, for example are any of the customer's directors DPIPs/FPPOs and, if so, do these DPIPs/FPPOs exert significant control over the customer or beneficial owner?
- 5.1.1.6. Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile bodies or individuals who are known to influence the government and other senior decision-makers?
- 5.1.1.7. Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?
- 5.1.1.8. Is the customer a financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations?
- 5.1.1.9. Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT/CPF obligations or wider conduct requirements in recent years?

⁷https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

- 5.1.1.10. Is the customer a public administration function or enterprise from a jurisdiction with low/high levels of corruption?
- 5.1.1.11. Is the customer's background consistent with what the bank knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?
- 5.1.1.12. Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as public procurement?
- 5.1.1.13. Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF/PF risk, such as non-profit organisations with weak AML/CFT due diligence controls?
- 5.1.1.14. Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?
- 5.1.1.15. Does the customer issue bearer shares or does it have nominee shareholders?

- 5.1.2. Product/services
 - 5.1.2.1. Which products are most utilised by high-risk categories of clients?
 - 5.1.2.2. Of the reports filed in terms of section 29 of the FIC Act, which products are more prone to abuse or can be noted as being susceptible for e.g. to fraud?
 - 5.1.2.3. Cash offerings e.g. deposits and ease of access/degrees of anonymity associated therewith.
 - 5.1.2.4. Which products allow for relative ease of access to cash
 - 5.1.2.5. Which products can be transacted with in such a manner that it is easy to lose audit trail to the beneficiary of the funds?
 - 5.1.2.6. Which products are most vulnerable to abuse according to observations within the bank?

- 5.1.3. Geographical risk
 - 5.1.3.1. The jurisdictions in which the customer is based or is resident.
 - 5.1.3.2. The jurisdictions that are the customer's main places of business.
 - 5.1.3.3. The jurisdictions to which the customer has relevant personal or business links, or financial or legal interests.
 - 5.1.3.4. Are the threats across the subsidiaries understood distinctly from another?
 - 5.1.3.5. Is the transactional activity and flow of funds from the bank to another and vice versa understood- i.e. inflows and outflows?
 - 5.1.3.6. Does the bank understand the destinations involved in the business of its clients?
 - 5.1.3.7. If goods are being exported- does the bank establish the final destination of the goods?
 - 5.1.3.8. Does the bank understand the customer's counterparty locations and if high risk jurisdictions are involved?
 - 5.1.3.9. Correspondent banking transactions- what trends can the bank identify from a risk perspective? (nostro and vostro accounts).
 - 5.1.3.10. Which countries does the bank often send funds to or receive funds from? Are there any noteworthy risks?
 - 5.1.3.11. Are there links to high-risk activity for certain client types/categories of clients?

- 5.1.3.12. Are specific locations connected with high levels of corruption/types of predicate offences/tax haven?
- 5.1.3.13. The nature and purpose of the business relationship, or the type of business, will often determine the relative importance of individual country and geographical risk factors. For example:
 - 5.1.3.13.1. Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant;
 - 5.1.3.13.2. Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, banks must consider to what extent this could be expected to or might give rise to suspicion, based on what the bank knows about the purpose and nature of the business relationship;
 - 5.1.3.13.3. Where the customer is a credit or financial institution, banks must pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision; and
 - 5.1.3.13.4. Where the customer is a trust or any other type of legal arrangement, or has a complex structure, banks must take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency and information sharing standards.

6. References

- 6.1. The following sources of information were consulted in the drafting of this guidance note and may be useful references when banks and controlling companies implement the guidelines and/ or requirements set out in this guidance note:
 - 6.1.1. FATF Guidance on the risk-based approach in the banking sector⁸;
 - 6.1.2. FATF Recommendations⁹;
 - 6.1.3. Austrac Insights on Assessing ML/TF Risks¹⁰; and
 - 6.1.4. the European Union Final Report on Guidelines on revised ML/TF Risk Factors¹¹.

⁸ <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

⁹ <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

¹⁰ <https://www.austrac.gov.au/sites/default/files/2020-08/AUSTRAC%20Insights%20-%20Assessing%20ML-TF%20Risk.pdf>

¹¹

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

7. Terminology

Term	Meaning
Foreign prominent public official	As per the definition contained in the FIC Act, a person referred to in Schedule 3B thereof.
Domestic Prominent Influential Person	As per the definition contained in the FIC Act, a person referred to in Schedule 3A thereof.
FATF Recommendations	As per the latest FATF Recommendations found at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html#:~:text=The%20FATF%20Recommendations,-Send&text=As%20amended%20March%202022.,of%20weapons%20of%20mass%20destruction.
Risk-based approach	A risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk (FATF) ¹²

8. Acknowledgement of receipt

- 8.1 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 5/2022, dated 15 June 2022.

¹² <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html>