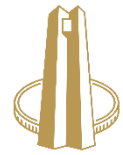
P O Box 427 Pretoria 0001 South Africa
370 Helen Joseph Street Pretoria 0002
+27 12 313 3911 / 0861 12 7272
www.resbank.co.za



SOUTH AFRICAN RESERVE BANK
Prudential Authority

Ref.: 15/8/1/2

G5/2024

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

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

Supervisory guidance for matters related to Business Risk Assessments and the assessment of money laundering, terrorist financing, and other unlawful activity

Executive Summary

The purpose of this guidance note is to inform banks and controlling companies (hereinafter collectively referred to as 'banks') of the Prudential Authority (PA)'s expectations related to banks' money laundering, terrorist financing, and proliferation financing (ML/TF/PF) business risk assessments and to assist banks and other relevant accountable institutions to enhance their understanding of ML/TF/PF risks in the context of their businesses.

Section 64A of the Banks Act, 1990 read with regulations 39, 50 and 36(17) of the Regulations relating to Banks (Regulations) requires every bank and controlling company 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 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, amongst 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 for the Banking Sector [1] indicates that a risk-based approach consists of two fundamental components namely, identifying ML/TF/PF risks and adopting mitigating controls that are commensurate with the ML/TF/PF risks identified to manage residual risks. The FATF indicates that when institutions assess risk, they should take appropriate steps to identify, assess, and understand the ML/TF/PF risks that may be present in their business activities and with their customers. In order to do so, institutions should produce a risk assessment that is commensurate with the nature, size, and complexity of their business.

1.2. The Financial Intelligence Centre Act 28 of 2001 (FIC Act) also outlines requirements for banks to have a risk management and compliance programme (RMCP) which enables the accountable institution to identify, assess, monitor, mitigate and manage the risk that the provision by the bank of products or services that may involve or facilitate money laundering activities or the financing of terrorist and related activities to ensure that they adequately identify, assess, monitor and implement preventive measures in addition to applying a risk-based approach as part of customer due diligence (CDD).

1.3. The PA acknowledges that in the context of an accountable institution's RMCP, 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. Building on the respective matters covered in Guidance Note 6 of 2022 relating to Business Risk Assessments (G6-2022), the PA decided to issue this guidance note to provide accountable institutions with further information related to general best practices for conducting a ML/TF/PF business risk assessment. The guidance note outlines how banks can identify the ML/TF/PF risks they are facing and determine how these risks are mitigated by the implementation of AML/CFT and counter-proliferation financing (CPF) controls. Through the correct application of the information contained in this guidance note, banks should be able to strengthen their business risk assessment process and improve the effectiveness of their RMCPs in accordance with financial crimes compliance (FCC) global standards[2] and adherence to their regulatory obligations.

2. Background on lessons learned from the ML/TF/PF Business Risk Assessment second thematic review

2.1. In September 2023, the PA finalised its second thematic review[3] of ML/TF/PF business risk assessments to determine whether banks demonstrated an improved understanding of ML/TF/PF risk from 2022 to 2023. Since the first thematic review was conducted, and throughout 2022 and 2023, significant progress has been made with respect to accountable institutions' understanding of ML/TF/PF risk and enhancing the quality of ML/TF/PF business risk assessments.

---

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

[2] For example, the Financial Action Task Force Standards

[3] The first thematic review was conducted by the PA in 2022

2.2. Specifically, the PA observed that banks improved in the following areas namely:

2.2.1. Enterprise- level ML/TF/PF risk assessment, a clearly articulated methodology, and assessment of entity-level inherent risks.

2.2.2. Banks produced consolidated enterprise-level ML/TF/PF risk assessments that were supported with risk assessment workpapers, reflecting calculations and internal data utilised to conduct the risk assessment exercise.

2.2.3. Banks developed business risk assessment methodologies outlining their approach to conducting the enterprise-level ML/TF/PF risk assessment. The business risk assessment methodologies generally referenced internal data utilised for conducting the risk assessment, specified an appropriate frequency for conducting a risk assessment, outlined circumstances that would trigger an off-cycle risk assessment, and described the stakeholders involved in the development and review of the risk assessment.

2.2.4. Banks identified standard inherent risk categories; however, banks were generally more thorough in identifying risks associated with their business model. Most banks identified broad categories of inherent risk and captured ML/TF/PF risks posed by their customers, products, services, delivery channels, and geographies.

2.3. The second thematic review also highlighted areas for further improvement that banks prioritise to strengthen their ML/TF/PF business risk assessments including the following:

2.3.1. Ensuring there are comprehensive assessment of AML/CFT/CPF controls.

2.3.2. Evaluating both the design and operating effectiveness of individual controls.

2.3.3. Assign weightings to controls based on the importance of that specific control.

2.3.4. Ensure that there are remedial actions undertaken where controls were highlighted as either not designed, not operating effectively, or did not exist.

2.3.5. Demonstrate how the residual risk score was calculated and evidence the use of both inherent risk and mitigating control scores when determining enterprise-level residual risk.

2.3.6. Calculate the residual risk score through calculations and detailed analyses and not relying only on the application of qualitative judgments.

3. Best practices for ML/TF/PF Business Risk Assessments

3.1. Purpose of a ML/TF/PF Business Risk Assessment

3.1.1. A ML/TF/PF business risk assessment is fundamental for providing a bank with a baseline understanding of the ML/TF/PF risks posed by customers, products, services, delivery channels, geographic locations and markets, and operations. The business risk assessment creates a roadmap that a bank should use for designing its RMCP and allocating resources to manage ML/TF/PF risks. The risk assessment helps to identify the nature and extent of ML/TF/PF risks so that an RMCP includes tailored and effective risk mitigating measures. An ML/TF/PF business risk assessment is also critical for identifying gaps or weaknesses in a bank's RMCP that can be addressed by introducing additional risk mitigation measures and reducing exposure to inherent risks.

3.2. Development of a ML/TF/PF Business Risk Assessment Methodology

3.2.1. As a first step, banks should clearly document a business risk assessment methodology that serves as a guide for carrying out their ML/TF/PF business risk assessments. At its core, risk assessment methodologies enable banks to determine their inherent ML/TF/PF risks, assess their internal control environment (both design and operating effectiveness), and ultimately derive their residual risk, which should be consistent with the bank's established risk appetite.

3.2.2. Generally, a business risk assessment methodology should include a purpose statement; the scope period for the risk assessment; the frequency at which risk assessments are performed; stakeholders involved in the risk assessment process (e.g. business, compliance); the design of a business risk assessment (e.g., the categories and associated weights for inherent risk factors and controls); and the process for deriving residual risk. The business risk assessment methodology should also cover the post-risk assessment process for obtaining senior management approval of the risk assessment, and any actions for tracking issues and remediating gaps identified through the risk assessment exercise.

3.2.3. The following list outlines best practices that banks can apply when developing the business risk assessment methodology.

3.2.3.1. The business risk assessment methodology should require the bank to update its risk assessment in response to changes in its customer base, products, services, delivery channels, and geographic locations and markets to ensure the risk assessment accurately reflects the institution's ML/TF/PF risks.

3.2.3.2. The business risk assessment methodology should define the assessment units in the risk assessment (such as by branch, business unit, or legal entity), which should cover the entirety of the banks' business.

3.2.3.3. The business risk assessment methodology should indicate how the bank utilises internal data and information that is both qualitative and quantitative in nature to conduct the risk assessment.

3.2.3.4. The risk assessment methodology should identify sources of data used for the business risk assessment, including accounting for any manual/scoring overrides applied for data issues or absences. Banks should decide what rating should be applied in instances where data cannot be easily sourced (e.g., answering "unknown" to certain questions may result in an automatic high-risk rating) and should consider remedial actions required to obtain the requested data.

3.2.4. Regarding assessing inherent risks, banks should understand the ML/TF/PF risks that may be present in their business activities and produce a ML/TF/PF business risk assessment that takes into consideration the following inherent risk factors:

3.2.4.1. Customer risk;
3.2.4.2. Product and service risk;
3.2.4.3. Delivery channel risk;
3.2.4.4. Geographic locations and market risk; and
3.2.4.5. Operational risk.

3.2.5. After assessing inherent risks, banks should identify the AML/CFT/CPF internal controls that mitigate and manage these ML/TF/PF risks, which can include the following:

3.2.6. Governance and Management Oversight:

3.2.6.1. Appropriate governance arrangements, including documented roles and responsibilities, escalation processes, approval protocols, and reporting to senior management and the Board of Directors.

3.2.7. Know Your Customer (KYC):

3.2.7.1. Customer ownership identification and verification, beneficial ownership identification and verification, developing an understanding of the nature and intended purpose of the business relationship, establishing a customer risk profile, and conducting ongoing CDD.

3.2.8. Internal Controls:

3.2.8.1. Suspicious activity monitoring systems and processes designed to identify potentially suspicious activity based on risk indicators, including unusual or unexpected activity or a change in a customer's profile.

3.2.8.2. Suspicious activity reporting, including procedures and processes in place to investigate and report suspicious activity in a complete, accurate, and timely manner.

3.2.8.3. Other internal controls that encompass policies, procedures, and processes related to regulatory reporting, recordkeeping, record retention, and information sharing.

3.2.9. Training:

3.2.9.1. Ongoing and role-based training for AML/CFT/CPF staff that provides all appropriate personnel with knowledge about AML/CFT/CPF regulations, internal policies and procedures, and evolving ML/TF/PF risks.

3.2.10. Independent Testing/Audit

3.2.10.1. Testing to evaluate the bank's RMCP policies and procedures, identify any critical gaps or issues, and implement stronger controls where required.

3.3. Report Drafting

3.3.1. Banks should develop a ML/TF/PF business risk assessment report that assesses ML/TF/PF inherent risks and mitigating controls to determine the accountable institution's residual risk. As part of the risk assessment exercise, banks should retain any workpapers utilised to collect data and calculate scores for the ML/TF/PF business risk assessment. Banks with multiple branches, legal entities, or business units may maintain sub-enterprise risk assessments across several assessment units; however, the results of these assessments should be presented in an enterprise-level risk assessment report.

3.4. Evaluating Inherent Risk

3.4.1. Inherent risk is the exposure to ML/TF/PF risk in the absence of any controls being applied. While there are a variety of ways to conduct a business risk assessment, banks are generally expected to evaluate the different levels of risk posed by their customers, products and services, delivery channels, geographic locations and markets, and operations. In addition to the factors mentioned in G6-2022, the following list outlines best practices that accountable institutions can apply to evaluate their inherent risks:

3.4.1.1. As part of each general inherent risk category, the business risk assessment should consider more granular risk factors and should assign each risk factor a score or weighting which reflects the level of risk associated with that risk factor and the prevalence of that risk compared to other risk factors. For example, a bank may consider customer risk as the most important contributor to AML/CFT/CPF risk because customers ultimately would be the point of introduction for any illicit proceeds, and as such, customer risk may be weighted more heavily than another inherent risk category.

3.4.1.2. The business risk assessment should reflect risk indicators that are applicable to the bank's business model. In identifying risk factors, the institution should include both quantitative risk factors (e.g., number of Politically Exposed Person ("PEP") customers, length of customer relationships, etc.) and qualitative risk factors (e.g., integration of new tools/systems) when selecting risk factors for each inherent risk category.

3.4.1.3. The bank should employ a standardised approach to assessing its inherent risk factors and utilise the same risk rating methodologies in the business risk assessment as it uses as part of its RMCP, if possible.

3.4.1.4. The bank, in performing its business risk assessment, should take into account ML/TF/PF risks associated with its local context, including risks specific to South Africa, by considering findings from the national and sectoral risk assessments.

3.5. Customer Risk:

3.5.1. Customer risk is based on the features of an accountable institution's customer base, including customers' professions, industries, and entity types, which can increase or decrease an accountable institution's ML/TF/PF risk. Banks should consider the following factors when evaluating inherent ML/TF/PF customer risk:

3.5.1.1. Customer or legal entity type;

3.5.1.2. Complex ownership and control structures of the customer;

3.5.1.3. Profession or industry (taking into account those sectors which may be vulnerable to ML/TF/PF abuse, such as accountants; lawyers; dealers in high value or precious goods; money services businesses, customers involved in export/import or shipping; and charities or other non-profit organisations);

3.5.1.4. PEP status or PEP exposure, including through beneficial owners, close associates, family members, and other related parties;

3.5.1.5. Length of customer relationship;

3.5.1.6. Regulatory status; and

3.5.1.7. Historical risk markers, such as being the subject of adverse media attention.

3.6. For customer risk, the bank should assign each customer type an inherent risk score (e.g., high, medium, low) or rating depending on the ML/TF/PF risk associated with that customer type. Each business unit can then determine the volume of customers for each customer type and apply this methodology to the other customer risk factors. This data can be utilised to assess each business unit's customer risk exposure—the percentage of each business unit that, for instance, has high, medium, or low-risk customers—and the accountable institution's overall inherent customer risk.

3.7. Product and Service Risk:

3.7.1. Product and service risk considers the products and services that a bank offers its customers and the characteristics of those products and services which can increase or decrease a bank's ML/TF/PF risk. Ideally, an enterprise-level ML/TF/PF risk assessment should enable a bank to understand how its product suite impacts its risk profile and identify which specific products and services contribute most to its overall risk. Banks should consider the following factors when evaluating inherent ML/TF/PF product and service risk:

3.7.1.1. Potential for intermediation: Whether the bank offers services that carry intermediated risk (e.g., the institution acts as an intermediary between two other financial institutions; the institution has limited visibility into the originator or beneficiary of a transaction that it is processing; or the institution relies on a third-party for information about an originator or beneficiary).

3.7.1.2. Use of potentially higher-risk medium of exchanges: Whether the accountable institution engages in potentially higher-risk mediums of exchange, such as through the use of cash, gold, or cryptocurrency asset service providers.

3.7.1.3. Potential for anonymity: Whether the bank offers services that facilitate anonymity and/or operate with limited transparency.

3.7.1.4. Easily transferable: Whether the bank offers products or services that can be easily transferred.

3.7.1.5. Cross-border funds flows: Whether the bank offers services that typically or characteristically involve the cross-border movement of funds.

3.7.1.6. Settlement times and terms: Whether the bank offers services that provide for near instantaneous and irrevocable settlement.

3.7.2. For product and service risk, the bank should review each product or service and assign an inherent risk score (e.g., high, medium, low) to the product or service based on the degree to which the product or service presents ML/TF/PF risk. Each business unit can then determine the volume of product or service types offered by the business, and the account balances or transactions involving that product or service. This data can be utilised to assess each business unit's exposure to that product or service (the percentage of each business unit's product or service that is rated according to the institution's risk classification) to determine the bank's overall inherent product and service risk. In assessing product and service risk, accountable institutions should also be aware of new or innovative payment services and technologies that may not be specifically offered by the institution but that utilise bank's services to deliver the product. Similarly, when there are new products and technologies to be adopted by an accountable institution, a risk assessment must take place prior to the launch of the product and utilisation of the technology.

3.8. Delivery Channel Risk:

3.8.1. Delivery channel risk is the extent to which the bank's methods of account origination or account servicing limits its understanding of the identity and activities of its customers and counterparties. Banks should consider the following factors when evaluating inherent ML/TF/PF delivery channel risk:

3.8.1.1. Employment of non-face-to-face channels and new technologies;
3.8.1.2. Involvement/delivery by or through a third party/intermediary; and
3.8.1.3. Near instantaneous or irrevocable settlement or processing (also a driver of product and service risk). For delivery channel risk, a business unit should determine the percentage of customers or accounts that are rated according to a bank's inherent risk score classification in order to determine the overall inherent delivery channel risk.

3.9. Geographic Location and Market Risk:

3.9.1. Geographic location and market risk is the extent to which an accountable institution is exposed to countries that present elevated ML/TF/PF risk through its transactions, operating locations and markets, customer base, and intermediaries. Banks should consider the following factors when evaluating inherent ML/TF/PF geographic location and market risk:

3.9.1.1. Transactional exposure: Locations where the institution has transactional exposure (i.e., volume of deposits by origin country).
3.9.1.2. Institutional exposure: Locations of the business division, business unit, or business line; location of a bank's subsidiaries, affiliates, intermediaries, and offices; and where the bank conducts business.
Customer exposure: Customers' domicile, incorporation, or nationality; and customers' primary place or business/headquarters.

3.9.2. Of significance, geographic location and market risk may also be assessed along with other risk factors in other inherent risk categories. To calculate geographic location and market risk, the business unit should calculate its transactional exposure (re, percentage of a business unit's transactions with specific countries), institutional exposure, and customer exposure and leverage the institution's geographic risk rating methodology when determining each country's risk rating.

3.10. Operational Risk:

3.10.1. Operational Risk is described by the Basel Committee on Banking Supervision as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events". In the context of AML/CFT/CPF, operational risk is the extent to which certain risk factors contribute to increasing the likelihood of failures in key controls through breakdowns in internal processes, people, or systems, or from external risk events. Banks should consider the following factors when evaluating inherent ML/TF/PF operational risk:

3.10.1.1. Customer base changes/turnover;
3.10.1.2. Launch of new products and/or services;

3.10.1.3. Adequacy and changes in core technology and systems;
3.10.1.4. Adequacy and changes/turnover of staffing and resourcing;
3.10.1.5. Recent projects and initiatives related to AML/CFT/CPF compliance matters (e.g., existence of backlogs of transaction monitoring alerts or CDD/KYC refreshes); and
3.10.1.6. Occurrence of risk events (e.g. enforcement actions, cyber threats impacting system functionality)

3.11. Evaluating Mitigating Controls

3.11.1. After inherent risks have been identified and evaluated, banks should assess their internal control environment to determine how effectively they mitigate the institution's ML/TF/PF risks. Mitigating controls include the bank's policies, procedures, and processes. The following list outlines best practices that accountable institutions can apply to evaluate their mitigating controls:

3.11.1.1. Each control area should be assigned a score that reflects the relative strength of that control as well as a weighting based on the importance that the institution places on that control, given the institution's overall risk profile and risk appetite. For example, a bank may decide to weight KYC the highest because its KYC controls might be its strongest preventative control against ML/TF/PF exposure, whereas training—albeit an important control—may have a comparatively lower weighting than KYC.
3.11.1.2. Banks should seek to map controls to specific inherent ML/TF/PF risk factors to ensure sufficient coverage of ML/TF/PF risks and should assess controls both for appropriate design and for operating effectiveness.
3.11.1.3. In the scenario that a bank determines that a mitigating control is not designed appropriately or functioning effectively, it should escalate this issue and create a remediation plan if a remedial activity is not already in progress.
3.11.1.4. Controls should be linked to key performance indicators, internal audit findings, and quantitative metrics when evaluating a control's overall effectiveness (such as if key performance indicators indicate significant issues or deficiencies with respect to specific controls).

3.12. Governance and Management Oversight:

3.12.1. Governance and management oversight are fundamental to oversee a bank's RMCP, implement AML/CFT/CPF controls commensurate with a bank's risk profile, and remain compliant with AML/CFT/CPF laws and regulations. An institution's governance function should ensure that:

3.12.1.1. A bank's documented RMCP is approved by the Board of Directors or an appropriate Board-level equivalent committee and is informed by the bank's ML/TF/PF risk assessment.
3.12.1.2. AML/CFT/CPF roles, responsibilities, and reporting lines are clearly documented across all three lines of defence.
3.12.1.3. The compliance function is led by individuals with sufficient background and expertise in AML/CFT/CPF.
3.12.1.4. The compliance function has the appropriate authority, independence, funding, staffing, information, and requisite technology to manage ML/TF/PF risks and fulfil the obligations of the RMCP.

3.13. KYC:

3.13.1. KYC is a bank's front line for defense against ML/TF/PF by adequately identifying and verifying the identities of current and prospective customers, including the purpose of their relationship and expected activity. Effective KYC enables banks to know who their customers are, what products and services of the accountable institution's they will use, and what types of transactions the customer is expected to conduct. Banks use this information to develop a customer's risk profile and conduct ongoing monitoring of the customer. Banks should also conduct enhanced due diligence measures on customers that pose elevated ML/TF/PF risk and ensure that all customer information is kept up to date, refreshing the customer's information according to certain risk-based intervals.

3.14. Internal Controls:

3.14.1. Internal controls typically consist of policies, procedures, and processes designed to mitigate ML/TF/PF risks associated with a bank's business and to ensure compliance with AML/CFT/CPF laws and regulations. A bank's internal controls include the following:

3.14.1.1. The risk assessment process informs the design of a bank's RMCP, enabling the bank to allocate resources and introduce mitigating measures to manage ML/TF/PF risks;
3.14.1.2. The suspicious activity monitoring programme consists of ongoing customer and transaction monitoring and, thus, informs the bank's suspicious activity reporting program;
3.14.1.3. Suspicious and unusual transaction reports; cash threshold reports; terrorist property reports; and information sharing is based on procedures and processes that a bank must have in place to investigate and report suspicious activity in a complete, accurate, and timely manner; and
3.14.1.4. The recordkeeping and record retention obligations require banks to maintain certain documentation and an audit trail of information that evidences the rationale and investigation which led to the filing of a suspicious and unusual transaction report; cash threshold report; or terrorist property report.

3.15. Training:

3.15.1. A comprehensive AML/CFT/CPF training program is critical to the overall effectiveness of an RMCP. Training should be provided on an ongoing basis and incorporate changes to AML/CFT/CPF laws and regulations, guidance, internal policies or procedures, and evolving ML/TF/PF risks. A comprehensive AML/CFT/CPF training program clearly documents expectations for:

3.15.1.1. New hire training;
3.15.1.2. Ongoing enterprise-wide training;
3.15.1.3. Board and senior management training; and
3.15.1.4. Targeted and role-based training.

3.16. Independent Testing/Audit:

3.16.1. Independent testing should be regularly performed by an internal audit department, external auditors, or other qualified and independent parties. The independent testing/audit function should report directly to the Board of Directors or a Board-level committee. Testing should be risk-based and should evaluate all operations, business units, and subsidiaries of a bank to identify gaps, deficiencies, and operational weaknesses in internal controls owned or overseen by the bank's business, operations, and compliance functions. Risk-based independent testing programs can vary depending on the accountable institution's size, complexity, business model, and risk profile, among other considerations. Ongoing reviews should be conducted concerning the effectiveness of remediation measures taken in response to the independent testing/audit function's findings.

3.17. Determining Residual Risk

3.17.1. Once the bank has evaluated both inherent risks and mitigating controls, the bank should determine its overall residual risk. Residual risk is the risk that remains after mitigating controls are applied to the total inherent risk (i.e., through the customers, products, services, delivery channels, geographies, and operational factors). Residual risk is calculated by balancing the level of inherent risk with the design and operating effectiveness of the accountable institution's internal control framework.

3.17.2. Residual risk indicates whether the ML/TF/PF risks within an accountable institution are being sufficiently managed. Residual risk enables a bank to pinpoint the nature and extent of ML/TF/PF risks in order to tailor its RMCP accordingly, focusing mitigating measures on the areas that pose the greatest risk. The outputs and findings of a bank's business risk assessment should, thus, be actionable, and wherever the results are different than expected, these discrepancies should be clearly explained.

3.17.3. Best practices indicate that banks should utilise a residual risk matrix that considers inherent risk and mitigating control ratings in order to generate a residual risk rating. Each bank can decide the type of risk matrix to adopt based on their respective business. Example risk matrices are below that range from a three-point scale to a five- point scale for assessing inherent risks, mitigating controls, and the resulting residual risks.

Inherent Risk Rating		Control Effectiveness Rating		
		Effective	Partially Effective	Ineffective
	High	**Medium**	**High**	**High**
	Medium	**Low**	**Medium**	**Medium**
	Low	**Low**	**Low**	**Low**

Inherent Risk Rating		Control Effectiveness Rating				
		Ineffective	Mostly Ineffective	Partially Effective	Mostly Effective	Effective
	Very High	**Very High**	**Very High**	**High**	**High**	**Medium**
	High	**High**	**High**	**High**	**Medium**	**Medium**
	Medium	**Medium**	**Medium**	**Medium**	**Low**	**Low**
	Low	**Low**	**Low**	**Low**	**Low**	**Very Low**
	Very Low	**Very Low**	**Very Low**	**Very Low**	**Very Low**	**Very Low**

4. Acknowledgement of receipt

4.1. Kindly ensure that a copy of this guidance note is made available to your bank. 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

Fundi Tshazibana
Chief Executive Officer

Date: 19/11/24

The previous guidance note issued was Banks Act Guidance note 4/2024, dated 8 July 2024.