Type:	*Policy Summary*
Name:	Money Laundering Control
Key search terms:	AML/ Sanctions/ Due Diligence/ Client Risk/ Terrorism Finance / Sanctions Screening/ AML Controls

1. Policy Statement

The business of Standard Bank Group Limited (the Group) is built on trust and integrity, and this vision is shared by our stakeholders; especially our clients, shareholders and regulators. An important element of trust and integrity is ensuring that the Group conducts its business in accordance with the Values and Code of Ethics that the Group has adopted, and in compliance with applicable laws, rules and standards. This summary describes the controls that need to be implemented to ensure that the Group and its products and services are not utilised for money laundering or terrorist financing purposes.

1 Policy Scope

This policy summary is designed to comply with applicable statutory and regulatory obligations across the Group; and applies to all entities and employees of the Group, regardless of location or business unit. This document reflects the Group's minimum requirements in respect of money laundering controls.

2 Purpose of this policy

Effective implementation of the policy will ensure the following:

- The risks arising from money laundering and terrorist financing (ML/TF) are mitigated and proactively managed;
- Relevant statutory and regulatory obligations are complied with;
- The Group and its employees are protected from legal, regulatory and reputational risks and/or administrative penalties that may result from instances or perceptions of ML/TF activity having taken place;

- The reputation and integrity of the Group is protected by taking all reasonable steps to prevent the products and services of the Group being used for ML/TF purposes;
- Client due diligence (CDD) principles, and the implementation of a risk-based approach to mitigation of ML/TF risks, are embedded as a cornerstone of the Group's business practices; and
- A framework is established that will enable the detection, investigation and reporting of suspicious activity and all other forms of reportable transaction to competent authorities.
- The Group aims to promote the principles of good governance by conducting regular reviews to test the effectiveness of its Risk Management and Compliance Programme (RMCP) and ensure compliance with this policy.

3 Roles and Responsibilities

The Group Board of Directors (by delegation to a Board committee or other appropriately empowered risk oversight body acting on the Board's behalf) and the boards of each of the Group's regulated subsidiary companies, ensures that an effective framework for managing ML/TF compliance risk is in place in the Group and subsidiary companies respectively.

The Group Board of Directors is accountable for ensuring compliance with the Risk Management and Compliance Programme (RMCP) and the relevant jurisdictional AML/CFT legislation. Group Compliance is responsible for ensuring compliance with the RMCP and the relevant jurisdictional AML/CFT legislation, by virtue of delegated responsibility from the Board of Directors.

It is prohibited to open and maintain anonymous, pseudonym, numbered accounts or accounts in obviously fictitious names, or to conduct a single or occasional transaction with an anonymous client. It is likewise prohibited to open accounts or enter into any relationship with shell banks, or open "payable through accounts".

The key minimum requirements that inform SBG's AML risk management approach can be summarised as follows:

- Client due diligence (CDD) must be conducted by obtaining and reviewing information about the client during the process of establishing a business relationship or concluding a single or occasional transaction with such client.

Where relevant, the nature of the business relationship and expected account activity will be ascertained. Source of funds information is obtained from all clients as part of the onboarding process;

- The documented CDD process will ensure that appropriate client identification and verification (CIV) is performed. The identity of any person acting on behalf of the client is established and verified in accordance with legal requirements, and reasonable measures are taken to establish and verify the identity of the beneficial owners for legal persons. Where the client is a legal arrangement such as a trust or a partnership, the onboarding process will involve gaining an understanding the ownership and control structure of that client.
- Where a beneficial owner cannot be identified through shareholding, information relating to individuals who exercise control over the client (controller), or individuals on whose behalf a transaction is conducted, must be obtained and verified;
- Sanctions screening must be performed on all clients, related parties and transactions in accordance with the requirements contained in the Group Financial Sanctions and Counter Terrorist Financing policy.
- Politically exposed persons (PEP's) screening must be performed on clients (or potential clients) and related parties to determine if they have a PEP status, or are family members or known close associates of a PEP;
- The ML/TF risk posed by all clients entering into a business relationship with Group entities must be assessed as part of the client on-boarding process, with due consideration to the following risk elements: (1) Products and services; (2) Distribution channel; (3) Client type; (4) Business activity/Occupation; (5) Jurisdiction.
- The CDD process facilitates the assignment of client risk rating, and the determination of the appropriate level of due diligence required. The information gathered must be kept up-to-date in order to manage the ML/TF risk throughout the client lifecycle effectively
- Where Group entities are not able to apply the appropriate level of CDD to an existing business relationship, processes to exit the relationship must be initiated, and filing of a suspicious transaction report (STR) or suspicious activity report (SAR) considered;
- Enhanced due diligence (EDD) requirements must be applied to clients identified as being high risk upon application of the Client Risk Assessment (CRA) scoring model. All foreign PEPs are automatically classified as high

risk. Where a business relationship with domestic PEPs is considered to be high risk, EDD measures must be applied;

- Ongoing due diligence of the client must be conducted to ensure that the identification and verification information relating to the client is still current and includes periodic and regular assessment against the relevant risk criteria in order to ensure that the risk rating of the client is still appropriate. This will include ongoing monitoring of the business relationship to ensure that the transactions are consistent with information held in relation to the risk profile and nature of the client's business;
- Group entities and their employees must report suspicious and unusual transactions/activities to the competent authorities in accordance with local regulatory requirements.
- Terrorist property reports, financial sanctions reports, cash threshold reports and cross-border funds transfer reporting, must be made in accordance with the regulatory requirements applicable to each jurisdiction in which the Group operates;
- Group entities must compile and maintain records of all Client acceptance and verification documentation for a minimum period of five years after the termination of the relationship with the Client, or in instances of a single or occasional transaction, such records must be kept for at least five years after the date of the single or occasional transaction
- Records should be kept in respect of information obtained in relation to source of funds and the nature of the business of the Client. Group entities should keep records of all transactions or activities that gave rise to the filing of a suspicious transaction report for a minimum period of five (5) years from the date on which the report was made to the relevant authority;
- The Group shall ensure that all relevant employees are trained on its AML/CFT Risk Management and Compliance Programme (RMCP) within one month of commencing employment within the Group, and where there is a subsequent change in an employee's role which requires specialised training. The Group shall ensure that all employees are made aware of any emerging ML/TF trends and methods by conducting awareness sessions regularly;
- Instances of non-compliance with the policy that constitute material Breaches of internal ML/TF controls must be reported to the relevant compliance committees, Business Compliance Officer (BCO) and Group Financial Crime Compliance in accordance with the existing reporting processes.

- Non-adherence to the controls may result in disciplinary action, with the possible consequence of dismissal.