Type:	*Policy Summary*
Name:	Money Laundering Control
Key search terms:	Money Laundering/ Financial Sanctions/ Due Diligence/ Client Risk/ Terrorist Financing/ Proliferation Financing/ Sanctions Screening/ ML/TF/PF Risk

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 to ensure that the group conducts its business in accordance with the values and Code of Ethics and Conduct that the group has adopted. The group has a zero-tolerance approach to wilful non-compliance with the Group Money Laundering Control policy, and/or relevant laws or regulations.

2 Policy Scope

The policy is designed to ensure that applicable statutory and regulatory obligations are complied with across the group. The policy applies to all entities and employees of the group, regardless of location or business unit.

3 Purpose of the Policy

The policy reflects the group's minimum requirements in respect of money laundering, terrorist financing and proliferation financing controls and must be supplemented with a local jurisdiction/group entity policy, procedure or related governance document, where more stringent legislative or regulatory requirements are in evidence.

Effective implementation of the policy will ensure the following:

- The risks arising from money laundering, terrorist financing and proliferation financing (ML/TF/PF) are identified, assessed, 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 penalties that may result from instances or perceptions of ML/TF/PF activity having taken place;
- The reputation and integrity of the group is protected by taking all reasonable steps to prevent the use of its products and services for ML/TF/PF purposes;
- Client due diligence (CDD) principles, and the implementation of a risk-based approach to mitigate ML/TF/PF 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 transactions and information requests to competent authorities.

The group aims to promote the principles of good governance by conducting regular reviews to test the effectiveness of its group-wide risk management framework and ensure compliance with the policy.

4 Roles and Responsibilities

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

Group Compliance is responsible for providing assurance to the group Board of Directors, that ML/TF/PF controls are adequate and operating effectively throughout the group.

5 Policy Requirements

The group 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, to open payable through accounts and to transact prior to the completion of CDD.

The key minimum requirements from the policy can best be summarised as follows:

- The nature and extent of ML/TF/PF risk exposure must be assessed in accordance with the Group Anti-Money Laundering and Counter-Terrorist Financing Risk-Based

Approach Framework by performing business risk assessments, client risk assessments, and product and services risk assessments;

- Controls that are proportionate to the level of ML/TF/PF risk identified must be developed, documented, maintained, implemented, and published in a Risk Management and Compliance Programme (RMCP). The RMCP must also provide for:
    - the method and manner in which the group entity will comply with its anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CTF/CPF) obligations
    - how the group entity will identify, assess, monitor, mitigate and manage the risk that the group entity's new and existing products or services may introduce ML/TF/PF vulnerabilities; and
    - how the group entity will assess and mitigate the ML/TF/PF risk introduced by prospective employees, current employees or persons that may influence employees;
- CDD must be performed during the process of establishing a business relationship or prior to concluding a single or occasional transaction with a client. The client information gathering process will facilitate the allocation of a client AML/CTF/CPF risk rating, and the determination of the appropriate level of CDD required. The information gathered must be kept up to date in order to manage the ML/TF/PF risk throughout the client lifecycle. The CDD steps include:
    - Identification – obtaining sufficient client information including identifying information on the client and its authorised persons and beneficial owners, the nature and purpose of a business relationship, the ownership and control structure of a client that is a legal person, trust or partnership, and the client's source of funds
    - Profiling – by performing ongoing politically exposed person (PEP) screening and risk management, and sanctions screening (in accordance with the Group Financial Sanctions/CTF/CPF Policy) on the client, and its related parties, beneficial owners and transactions. The client ML/TF/PF risk rating is then determined with due consideration to the results of screening and the client type, business activity/industry or occupation, jurisdiction, products and services, and distribution channel;
    - Verification – by taking reasonable risk-based measures to verify client information and/or obtain additional (that is, simplified, standard or enhanced due diligence); and
    - Ongoing due diligence – by conducting risk-based periodic or points of significant interaction reviews to ensure that client information remains current and relevant,

and ongoing transaction monitoring to ensure that subsequent transactions are consistent with the client information on record. When client information changes, the profiling and verification steps must be repeated;

- Where the client or related party to the client has been designated as a high risk PEP, the client's source of wealth information must also be established and corroborated. Foreign PEPs are automatically classified as high-risk. Domestic PEPs with adverse media information and high client-risk scores are classified as high-risk;
- Senior management approval must obtained when entering into or continuing with any high-risk business relationship;
- Group entities that are not able to conduct the appropriate level of CDD on an existing business relationship must initiate processes to exit the relationship, and consider filing a suspicious transaction or activity report;
- Group entities and their employees must report suspicious and unusual transactions/activities to competent authorities in accordance with jurisdictional regulatory requirements. Terrorist property, cash or currency threshold, electronic or wire transfers and cross-border cash conveyance reporting, as well as requests or instructions received from competent authorities must be submitted or addressed 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 information and transactions for a minimum period of five years after the termination of a business relationship with the client. 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 of ML/TF/PF regulatory reports and information requests should also be kept;
- The group must maintain appropriate controls to protect the confidentiality of client information, and to comply with all relevant jurisdictional data privacy laws.
- The group shall ensure that all relevant employees receive generic AML/CTF/CPF training within one month of commencing employment, and appropriate role specific specialised training. The group shall ensure that all employees are made aware of any emerging ML/TF/PF trends and methods by conducting regular awareness sessions; and
- Material breaches of internal ML/TF/PF controls and regulatory non-compliance must be reported to the relevant compliance committees, the designated group Compliance Officer, and Group Financial Crime Compliance in accordance with the existing governance processes.

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