AML/CFT RISK BASED SUPERVISORY FRAMEWORK AND MANUAL

JUNE 2019

T. Chinamo
Chief Executive Officer

Vision

To be a world-class regulator of diverse, efficient, lucrative and secure capital markets underpinned by strong Securities Market Intermediaries (SMI)

Mission

To protect investors through the provision of an optimal regulatory environment that promotes fairness and the sustainable development of the capital markets for national economic growth

Core Values

***F**airness*: We are just and impartial in all our decisions and actions. We are consistent and transparent in our conduct.

***A**ccountability*: We account for the authority and resources entrusted to us. We take full responsibility for our decisions and actions.

***C**ompetence*: We continually upgrade our skills and competences to keep abreast with market developments and best practices. We are innovative and maintain the cutting edge in all we do.

***I**ntegrity*: We are honest and uphold the highest standards of professionalism. We can be trusted to keep privileged information confidential. We can be relied upon by all stakeholders.

***T**eaming*: We are a cohesive and high performing team that executes and delivers break through results.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AML/CFT	Anti-money laundering/Countering the financing of terrorism
CDD	Customer due diligence
EDD	Enhanced due diligence
FAFT	Financial action task force
FIU	Financial intelligence unit
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
ML	Money laundering
PEP	Politically-exposed person
RBS	Risk-based supervision
SECZ	Securities and Exchange Commission of Zimbabwe
SII	Supervisor-In-Charge of Inspection
SLO	Supervision and Licensing Officer
SMI	Securities Market Intermediary
SSD	Supervision and Surveillance Department
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations

AML/CFT RISK-BASED SUPERVISION FRAMEWORK

1. INTRODUCTION

This policy framework sets out the Securities and Exchange Commission (SECZ)'s AML/CFT risk-based approach to supervision of Securities Market Intermediaries (SMIs). Risk based approach (RBA) is central to the effective implementation of the Financial Action Task Force (FATF) Recommendations. The main objective of the AML/CFT risk-based supervision (RBS) framework is to provide an effective process to evaluate methods adopted by SMIs in the securities sector to identify and assess money laundering and terrorist financing risks to which they are exposed and to ascertain the appropriateness of their AML/CFT risk mitigation strategies. This is in line with Zimbabwe's international obligations and the country's commitment to play its part in the national, regional and global fight against money laundering and terrorist financing. This is achieved through:

i. Assessing the existence and adequacy of SMIs' AML/CFT policies and procedures;
ii. Evaluating the effectiveness of SMIs' KYC/CDD standards;
iii. Assessing management processes to identify, measure, monitor and control AML/CFT risks;
iv. Evaluating the SMIs' suspicious and large cash transactions reporting standards;
v. Assessing SMI's systems of maintaining proper record of transactions;
vi. Assessing SMIs' compliance with relevant Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) directives, rules and laws and the effectiveness of SMIs' compliance procedures;

vii. Communicating AML/CFT related findings, directives, and recommendations in a clear and timely manner, and obtaining commitments by board of directors and management to correct significant deficiencies;

viii. Ensuring that all the AML/CFT deficiencies are fully and timely rectified in an appropriate manner;

ix. Providing guidance on AML/CFT best practices;

x. Facilitating AML/CFT related training and development and assessing the effectiveness of their own internal AML/CFT training.

Under the AML/CFT RBS approach, the focus is on identifying and assessing ML/TF risks and supervising institutions in a manner that is commensurate with the risks and taking necessary action that leads to compliance by regulated entities. This approach enables the Commission to prioritize the use of its resources by allocating them according to individual SMIs' ML/TF risk profiles.

Development of the AML/CFT supervisory framework is a dynamic process due to continuous changes in the securities industry both locally and globally. Accordingly, SECZ shall continue to review this framework from time to time to ensure that it remains relevant and effective.

2. RATIONALE FOR THE AML/CFT RISK BASED SUPERVISION APPROACH

The risk-based approach to AML/CFT entails that the Commission should first identify and assess AML/CFT risks to which the SMIs are exposed, determine which of the SMIs present greatest risks and direct greater supervisory effort and resources towards such high risk SMIs, while making resource savings in areas of lower risk. This new approach was necessitated following an update by the FATF on its recommendations to strengthen global safeguards and further protect the integrity of the financial system by providing stronger tools to act against financial crime.

The AML/CFT RBS emphasises the need for an understanding by SMIs' of the ML/TF risks they face as well as specific products and services, customer base, the capacity in which their customers are operating (e.g. on their own behalf or on behalf of underlying customers), jurisdictions in which they operate, and the effectiveness of risk controls put in place. It also puts it upon SECZ to maintain an understanding of the ML/TF risks specific to the SMIs' it supervises, and the degree to which AML/CFT measures can mitigate such risks.

AML/CFT RBS overall ensures the identification of ML/TF risks and the definition and adoption of risk-sensitive measures that are commensurate with the ML/TF risks identified.

3. CLASSIFICATION OF SMIs AND DETERMINATION OF SCOPE OF INSPECTION

SMIs shall be classified according to the level of ML/TF risk they pose, high, moderate or low. The classification and scope of inspection is as indicated in Table 1.

Table 1: Classification and determination of scope

OVERALL COMPOSITE ML/ TF RISK	SCOPE	
	FULL SCOPE	TARGETED
HIGH	12 MONTHS	ADHOC
MODERATE	24 MONTHS	ADHOC
LOW	36 MONTHS	ADHOC (but limited)

4. RESPONSIBILITY FOR SUPERVISORY ACTIVITIES

The Head of Supervision and Surveillance Department (SSD) shall oversee all the supervisory and Surveillance functions and quality assurance. Manager: Supervision and Licensing shall be responsible for carrying out the supervisory and licensing activities. AML/CFT Supervision of all SMIs shall be under Supervision and Surveillance Department.

For each inspection, there shall be at least two AML/CFT inspectors. Each team of inspectors shall be headed by a Supervisor responsible for the inspection i.e. the Supervisor In-charge of Inspection (SII). The Supervision and Licensing Officer (SLO) will be the appointed contact person for the SMI under inspection.

5. KEY RISKS FOR CONSIDERATION

The Commission assesses ML/TF risks to which the securities sector is exposed, and the ML/TF risks associated with SMIs' both at an individual firm level and within the securities subsectors in which they operate. The risks may be related to each other in some respects and may change as the capital markets develop. This therefore requires the need for the adoption of the risk-based supervision as a dynamic process. The risks for consideration are as described below;

Table 2: Risk descriptions

	RISK DESCRIPTIONS[1]
Money laundering (ML) risk	The risk that a country, financial institution or business unit could be used for ML.
Terrorism-financing (TF) risk	The risk that a country, financial institution or business unit could be used for TF. While in many respects this is similar to ML risk, TF risk has features that may be different
Compliance risk	This refers to the current and prospective risk of damage to the organisation's business model or objectives, reputation and financial soundness arising from non-adherence with regulatory requirements and expectations of key stakeholders such as clients, staff members and the society as a whole. Compliance risk is an institutional -level concern and revolves around non-adherence with AML/CFT regulatory requirements. Compliance risk is a key driver in implementing AML/CFT controls and the risk management approach of institutions depends on several variables.
Risk of exclusion	Uncertainty associated with large, informal and primarily cash economies that are not typically subject to any AML/CFT measures and which obscure information about the informal financial sector and underlying transactions. For example, a remittance sender is excluded from sending a remittance due to a lack of documentation and then utilises an informal cross-border remittance service linked to unknown intermediaries.
Illicit financial flows risk	This is the risk that institutions are used as channels for money that breaks laws in their region, transfer and use. This normally goes beyond laundering to include tax evasion, transfer mispricing, corruption and trade mispricing thereby compromising financial integrity

6. ELEMENTS OF A SOUND AML/CFT RISK MANAGEMENT SYSTEM

While risk management systems vary among SMIs, there are four basic elements contributing to a sound risk management environment.

(i) Active Board and senior management AML/CFT oversight;

(ii) AML/CFT organisational policies and procedures that have been developed and implemented to manage business activities effectively;

(iii) Adequate AML/CFT management information systems (MIS) that support all business activities; and

[1] For purposes of simplicity, the above risks shall all be referred to as ML/TF risks

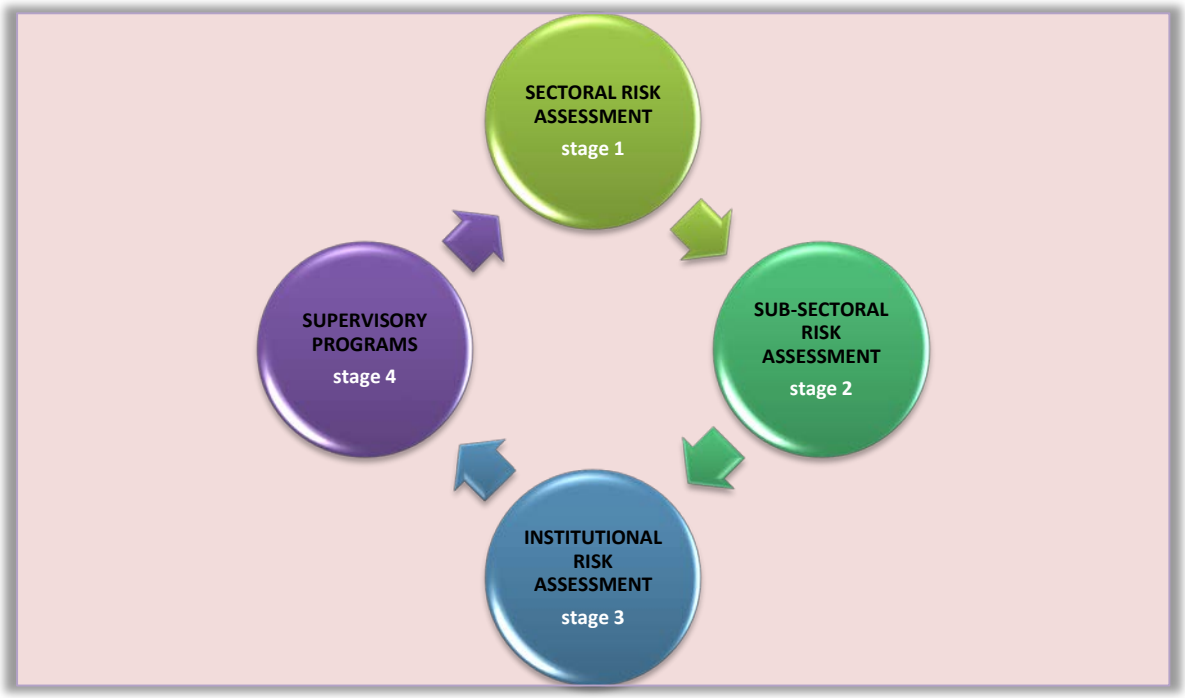
(iv) Established internal controls supported by periodic comprehensive audits that detect any deficiencies in the internal control environment in a timely fashion.

All sound risk management programs regardless of their design, have several common fundamentals. A typical risk management process should include risk identification, measurement, control and monitoring.

7. AML/CFT RISK BASED SUPERVISION METHODOLOGY

AML/CFT risk-based supervision is an ongoing process that is cyclical in nature whereby ML/TF risks of SMIs are assessed and appropriate supervisory plans are designed and executed in an efficient manner. Four broad processes inform the AML/CFT RBS Framework, namely Sectoral risk Assessment, Sub-sectoral risk assessment, Institutional risk assessment and Supervisory programs. These are as depicted in figure 1.

Figure 1: AML/CFT RBS Framework



7.1. SECTORAL RISK ASSESSMENT

Risk based supervision is primarily informed by sectoral risk assessment, a process which is broad in nature. This process is significant in determining the categories of licensees to which more supervisory resources should be dedicated. The process should be conducted at least annually in order to keep the regulator updated on categories of licensees posing high ML/TF risk.

The Commission shall use an in-house tool that mirrors the World Bank Tool's Securities Sector Vulnerability Module 4, for risk assessment to conduct sectoral analysis and is subject to replacement should the Commission acquire/develop better models for the risk assessment. The analysis shall initially consider inherent ML/TF risks of each category of licensees and then evaluate the control measures in place from an umbrella perspective. The residual risk for each category will be determined and these categories of licensees will be ranked according to the level of residual risk from the highest to the lowest. As an example, the Asset Management category may rank first, the dealing firms second and the Advisory firms last.

Data for the analysis shall be extracted from various sources including questionnaires, quarterly AML/CFT returns and any other relevant sources. This analysis will then determine the level of supervisory effort that the Commission should place on each license category.

7.2. SUB-SECTRORAL RISK ASSESSMENTS

Sub-sectoral risk assessments shall be conducted on a quarterly basis and shall inform the selection of the specific institutions in each category to dedicate more supervisory resources. The Sub-sectors include Securities Exchanges, Securities Dealing firms, Securities Custodians, Securities Transfer Secretaries, Securities Investment/Asset Management Firms and Securities Investment Advisors. The

process shall be conducted giving reference to the results of the last sectoral risk assessment.

The analysis shall be based on both inherent vulnerability factors and the AML/CFT controls the institutions have in place to reduce ML/TF risk. Data for the analysis shall be extracted from standard quarterly returns submitted to the Commission. The quarterly inherent risk assessments shall be based on the following factors:

a) Clients

For purposes of assessing money laundering risk inherent in SMIs client base, the SLO shall consider factors such as the proportion of clients who are politically exposed, non-resident,non-govermental organisations and high net worth. Additionally, the SLO shall also establish whether there are any clients with criminal backgrounds or clients with links to people with criminal backgrounds. The SLO shall also establish if SMIs have trust accounts in their client base and if the SMIs have access to beneficial ownership information amongst other relevant factors.

Every variable considered shall be given a weighted risk score in order to determine the overall score for “client” inherent risk.

b) Products and services

The SLO shall consider factors such as the size of SMIs relative to the industry, product diversity, product complexity, existence of deposit features and liquidity of portfolios amongst other factors. These factors shall also be awarded weighted risk scores to determine the overall risk inherent in SMIs products and services.

c) Delivery channels

Some delivery channels/servicing methods can increase money laundering risk because they increase the risk that the SMI under review does not truly know or understand the identity and activities of its clients. Consequently, it should be assessed whether, and to what extent, the method of account origination or account servicing, such as non-face-to-face account opening or the involvement of third parties, including intermediaries, could increase the inherent money laundering risk. Through such analysis the SLO should then be able to determine the overall inherent channels risk.

d) Geography/Country

Identifying geographic locations that may pose a higher risk is a core component of any inherent risk assessment. The SLO should seek to determine and evaluate specific risk associated with the SMI doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations. The SLO should also determine the number of the SMI's clients within each country basing on either domicile, incorporation or nationality.

Geography/Country risk should be considered together with some of the other risk factors in other risk categories, such as in clients of the SMI and in its products/services. For example, the percentage of the SMI's business transactions with a high-risk country may provide an indication of the inherent risk from a Geography/Country perspective.

Geography/Country risk will be important in any Sanctions Risk Assessment, not only with respect to sanctioned countries themselves, but also those which may have well known/important links or other significant connections to sanctioned countries. These could include countries bordering, or in close proximity to, sanctioned countries, or those countries

which present potential opportunities for the diversion of funds with the intent to violate or circumvent sanctions regulations.

Additionally, Geography/Country risk will also be applicable in any Anti-Bribery and Corruption Risk Assessment. Certain jurisdictions carry increased levels of bribery and corruption risk, usually to do with how those in power are able to abuse their positions for their own financial gain. Where such jurisdictions are present in a SMI, the bribery and corruption risks need to be appropriately reflected. A risk score should then be determined for the geography risk factor.

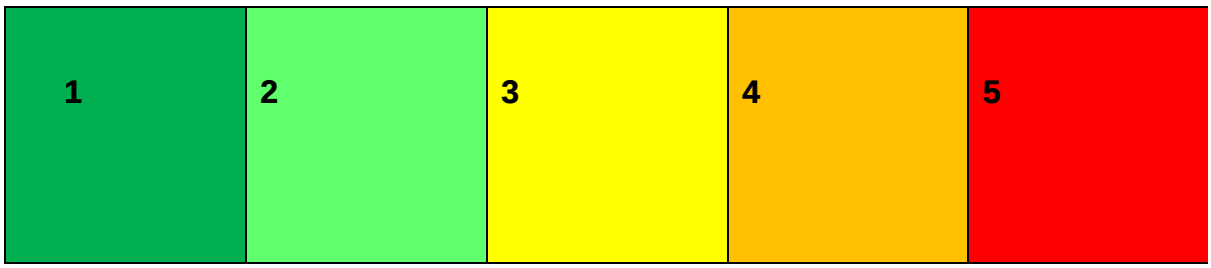
e) Other qualitative risk factors

Additional risk factors can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML controls. Qualitative risk factors directly or indirectly affect inherent risk factors. For example, significant strategy and operational changes, such as the introduction of a major new product, or service, a merger or an acquisition, opening in a new location or closing an entity may affect the inherent risk. These changes may well require a review of existing, or the establishment of new, internal controls, and may probe the SLO to assess whether the inherent risk for the SMI has been increased or changed.

Other qualitative risk factors might include; Client base stability, Integration of IT systems, expected account/client growth, expected revenue growth, recent AML compliance employee turnover, reliance on third party providers, recent/planned introductions of new products and/or services, recent/planned acquisitions, recent projects and initiatives related to AML compliance matters, recent relevant enforcement actions and national risk assessments.

The risk scores shall range between 1 and 5, with 1 representing the least risk and 5 representing the highest risk. The scores and the colour codes are as indicated in figure 2.

Figure 2: Risk rating scale and colour codes



1=Low, 2=Medium Low, 3=Medium, 4=Medium High, 5=High

7.3. INSTITUTIONAL RISK ASSESSMENT

The Commission should ensure that all SMIs conduct their own Institutional ML/TF risk self-assessments. The procedures adopted and the results thereto should be documented, and such reports should be shared with the Commission. Institutional risk self-assessments should be conducted at least annually and submitted to the Commission three months before year end.

SMIs should determine their level of inherent risk by looking at factors as indicated in section 7.2 amongst others which they deem relevant. AML/CFT

control measure should also be evaluated in terms of their availability and effectiveness. The institutions should then determine the level of ML/TF residual risk that they face.

7.4. SUPERVISORY PROGRAMS

The supervisory programs shall be influenced by results from the Sub-sectorial risk assessments. Focus will be given to institutions ranking higher on inherent ML/TF risk. The supervisory programs framework involves understanding the institution's profile, planning and scheduling AML/CFT supervisory action, defining AML/CFT onsite inspection objectives, performing onsite inspection, follow up and monitoring. Table 3 shows the stages and the necessary documentation that must be prepared.

Table 3: Supervisory programs framework

	STAGES	OUTPUT
1	Understanding the SMI and its risk profile	1.SMI Profile
2	Planning and scheduling AML/CFT supervisory action	2. Supervisory plan
3	Defining AML/CFT On-site Inspection Objectives and Activities.	3. Scope Memorandum
4	Performing ML/TF On-site Inspection	4. Inspection Report
5	Follow-up and Monitoring	5. Supervision Reports 6. Updated SMI Profile

7.4.1 Understanding the SMI and its risk profile

The first step in the AML/CFT supervisory program is to develop a good understanding of the SMI being supervised. The focus should be on understanding the institution in terms of history, vision, strategic objectives and other factors shown in Appendix 1, institutional soundness and whether there is any area of concern (overall assessment of the institution); outcomes of past

assessments, outcome of analysis of off-site examination, amongst others. The aim is to develop an institutional profile which helps in putting together an appropriate supervisory strategy for the institution.

The institutional profile also assists in understanding additional issues of importance to RBS: culture, operating and business model, management practices, risk profile, institutional risk appetite as well as other unique institutional characteristics. The institutional profile is not static and is constantly updated to reflect corresponding changes at economy, sector and institutional level. This step is critical in tailoring the supervision plan to meet the characteristics of the SMI and adjusting that plan on an ongoing basis as circumstances change.

A comprehensive and up-to-date SMI profile should be maintained for every supervised SMI and this is the responsibility of the Supervision and Licensing Officer responsible for the SMI. The SMI profile should reflect the current AML/CFT risk profile of an SMI. At a minimum it should be updated quarterly. It is necessary for management to subject SMI profiles to random checks to ensure consistency in quality and completeness.

7.4.2. Planning & scheduling supervisory action

The Supervisory Plan represents a bridge between the SMI's risk assessment, which identifies significant ML/TF risks and supervisory concerns, and the supervisory activities to be conducted. A comprehensive supervisory plan should be prepared for each SMI (by the Officer) annually and updated as appropriate. The plan should demonstrate that supervisory concerns identified through the AML/CFT risk assessment process and the deficiencies noted in the previous inspection are being or will be addressed. To the extent that the SMI's risk management systems are adequate, the level of supervisory activity may be adjusted.

The planning horizon to be covered by the plan is generally 12 months. The plan should generally address all supervisory activities to be conducted, the scope of those activities (full or targeted); the objectives of those activities (e.g. review of specific business lines, products, support functions, legal entities); and specific concerns regarding those activities, if any.

The different supervisory techniques that may be applied include:

Off-site examination: this involves ML/TF off-site monitoring of the SMI's performance and condition together with progress on implementation of various directives and/or recommendations from the supervisor. This is achieved through submission and analysis of AML/CFT quarterly returns.

Full scope on-site inspection: a full scope ML/TF on-site inspection is one that is comprehensive in scope to assess the adequacy and effectiveness of the SMI's AML/CFT framework.

Ad hoc inspection: Prompt ML/TF on-site inspections, usually limited in scope, are designed to test a specific area of supervisory concern e.g. compliance with laws and regulations, etc...

Liaison with home/host supervisors: correspondence or visits to the home/host supervisors to obtain further information or to discuss supervisory issues or actions that might be taken by the appropriate supervisors. This also includes other local supervisory bodies.

Supervision & Surveillance Department (SSD) Pre-inspection Time Line…

The pre-inspection planning effort may be accomplished using both on-site and off-site data. As a general guide, the Commission arranges for SMI management to complete and submit the **Pre-Inspection Questionnaire** (PIQ) approximately

30-45 days in advance of the inspection. Details of the pre-inspection timeline are summarized in Table 4 for easy reference.

Generally, inspections should be scheduled according to the approved supervisory strategy.

Table 4: Pre-inspection Time Line

DATE	REQUIRED ACTIVITY
Day 1	Dispatch PIQ
Day 15	Receive completed PIQ from subject SMI
Day 16 to 19	Review completed PIQ submitted by SMI
Day 20	Submit pre-inspection plan & preliminary assessment to Manager –SSD
Day 22	Submit tentative plan, preliminary risk assessment and scope memorandum to the Head of SSD
Day 23	Dispatch letter requesting AML/CFT meeting to SMI management
Day 25	Conduct pre-inspection AML/CFT meetings with SMI management
Day 26 to 29	Conduct on-site review of sensitive information such as board minutes and strategy documents
Day 30	Commence on-site inspection of the SMI

7.4.3. Defining on-site inspection objectives and activities

The SII shall prepare an on-site inspection timeline for the forthcoming inspection and request information from the SMI for the purpose of conducting preliminary review and preparing a Scope Memorandum. The Scope Memorandum identifies key objectives and the scope of an on-site inspection. A letter introducing inspectors to be involved in the inspection exercise should be sent to the SMI. The SMI should be informed at least one week prior to commencement of examination. Sample Introduction letter is presented in the RBS Manual.

An inspection timeline is a tool that guides the whole process from planning to completion of an on-site inspection, including responses to the report of

inspection from the inspected SMI. It specifies time periods within which specified activities should be completed by the individuals concerned. A sample of the on-site inspection timeline and guidance for preparation are presented in the RBS Manual.

The **Information Request Letter** identifies the information necessary for the successful execution of the on-site inspection procedures. It is important that the information request letter be tailored to fit the specific characteristics and risk profile of the SMI to be examined and the scope of the activities to be performed. Thus, the effective use of the information request letter is highly dependent upon the planning and scoping of a risk-based inspection. To eliminate duplication and minimize the regulatory burden on an SMI, the letter should not request information that is provided on a regular basis to or that is available within SECZ, such as regulatory reports and other financial information.

In the course of preparing the Scope Memorandum, the SII will coordinate Preliminary Review, both on-site and off-site, including pre-inspection meetings with senior management of the SMI. The pre-inspection meeting entails a general discussion of major concerns arising from off-site and pre-inspection reviews.

The AML/CFT **Scope Memorandum** is an integral product in the risk-based methodology as it identifies the key objectives and scope of the on-site inspection. The focus of on-site inspection activities, identified in the scope memorandum, should be oriented to a top-down approach that includes a review of the SMI's internal risk management systems and an appropriate level of transaction testing. The Scope Memorandum should be tailored to the size, complexity and current rating of the SMI and should define the objectives of the inspection. The Scope Memorandum should be submitted to SSD Management for authorization.

The Supervisor-in-charge of Inspection should prepare an introduction letter indicating the objectives and scope of the inspection, staff to be involved,

commencement and completion dates. The SMI should be informed at least one week prior to commencement of the inspection.

7.4.4. Performing on-site inspection

a) Inspection Entrance Meetings

At the beginning of each inspection, an Inspection Entrance Meeting should be held. The purpose of the meeting is to formally commission the inspection, indicate scope and focus of the inspection, highlight previous inspection concerns; explain how inspectors will conduct the inspection; provide details on the roles of participating inspectors; and respond to any questions from the SMI.

b) Inspection Procedures

The major areas that should be looked at during the inspection can be categorised into five main sections. It is however important to note that these categories are not exhaustive, and the inspection team can broaden the scope in whichever way they see fit.

Each factor is assessed for overall design and operating effectiveness and may be rated according to a pre-defined rating scale or based on qualitative factors, e.g. ‘satisfactory’, ‘needs improvement’ or ‘deficient’. These are as discussed below.

Customer due diligence and Know Your Customer Principles

Customer due diligence (CDD) and Know Your Client (KYC) are key elements in the fight against money laundering and terrorist financing. These elements enable SMIs to know their customers and understand their financial dealings better, which in turn help identify suspicious transactions and manage ML/TF risks prudently.

During inspections, SII should ensure that SMIs exercise CDD through identifying, verifying and monitoring all aspects of the applicant’s identity,

residential address, any temporary address, and information on the source of funds and the source of wealth. This should also include information relating to any beneficial owner who has an interest in the securities, or controller who exercises influence over the investment.

SII should verify whether CDD has been performed for all business relationships being established. This is enabled through checking the availability of identification documents of every customer and beneficial owner and information on the purpose and intended nature of the business relationship. It is also important to ensure that CDD has been conducted according to the SMIs ML/TF risk classification of the respective clients.

For **low risk** clients, it is acceptable that SMIs perform simplified/reduced due diligence. Acceptable proof of address for these customers include, but are not limited to letter from employers, referral letters from senior bank officials, affidavits from landlords and letters from schools, chiefs and head man.

SII should also ensure that enhanced due diligence (EDD) has been performed for **higher risks** clients including non-resident customers, customers from countries that do not or insufficiently apply the FATF standards, high net worth individuals, politically exposed persons (PEPs), non-face-to-face customers, customers with dubious reputation as per public information available, the use of front entities of entities, entities with complex corporate structures, unregistered and unlicensed investment vehicles and cross-border omnibus and correspondent accounts amongst others.

Other considerations that should prompt EDD include whether the client is sanctioned by and relevant competent authority for non-compliance with AML/CFT laws and is not engaging in remediation to improve its compliance. EDD should also be performed for customers who reside in or whose primary

source of income originates from high risk jurisdictions, customers who have sanction exposure and those that have non-transparent ownership structures.

The EDD process includes enquiries on the purpose for opening an account, the level and nature of trading activities intended, the ultimate beneficial owners, the source of funds and senior management's approval for opening the account/s of corporates. The SII should ensure that this information is available for clients that have been categorized as high-risk clients by the SMI.

The SII should also ensure that the SMI is conducting CDD on an ongoing basis. Ongoing CDD should be conducted on a periodic basis depending on the risk classification of the SMIs clients. As a minimum, re-verification should be done on an annual basis for high risk clients, after every 2 years for medium risk clients and after every 3 years for low risk clients.

Ongoing CDD should also be trigger based and such triggers include instances when there is suspicion of ML/TF, a transaction of significant value takes place, customer documentation standards change substantially, there is a material change in the way the account is being operated and when the SMI becomes aware that it lacks sufficient information about an existing customer.

The SII should also verify if all clients of the SMI are screened against the sanctions lists that are prescribed in the SMI's sanctions procedure. These lists include World Check, OFAC, UN and EU amongst others. The client acceptance policy of the SMI should specify the onboarding procedures of sanctioned individuals or entities and the SII should ensure onboarding of such clients is done in accordance with the policy.

Internal Controls, Policies & Procedures

The internal controls, policies and procedures should be evaluated in terms of their availability, adequacy and whether they are being effectively implemented. It is necessary to ensure that these internal controls, policies and procedures cover proper management oversight systems and controls, segregation of duties, training and other related matters and that the policies and procedures are approved and signed by the board.

As a minimum, each SMI should have AML/CFT policies and procedures including the KYC policy and other considerations relating to AML/CFT, some of which are explained in the subsequent headings. The KYC policies and procedures should incorporate four key elements; customer Acceptance Policy, Customer Identification Procedures, Monitoring of Transactions and Risk Management. What to look out for under these elements is as stipulated in the AML/CFT Guideline for the Securities Sector.

The AML/CFT policy should cover the appointment of a Compliance Officer/Money laundering reporting officer (MLRO) whose responsibility is to monitor and report all suspicious transactions, overseeing and ensuring compliance with regulatory guidelines on AML/CFT issues from time to time, developing appropriate compliance management arrangements across the full range of AML/CFT areas, and maintaining close liaison with the Securities and Exchange Commission and other designated institutions involved in the fight against money laundering and combating financing of terrorism.

The AML/CFT policy should also cover Client due diligence procedures including ongoing due diligence, monitoring and management information systems, reporting procedures for suspicious and unusual transactions, record keeping procedures as well as training and awareness programmes. The

AML/CFT policy should outline the roles and responsibilities of the board in ensuring that the policies are effectively implemented.

The SMI's internal audit and compliance function should provide an independent evaluation of the SMI's policies and procedures, including legal and regulatory requirements. The SLO responsible for the inspection should therefore ascertain whether the audit machinery is staffed adequately with individuals who are well versed with such AML/CFT policies and procedures.

Reporting of Suspicious Transactions

The inspection should ensure that submissions of STRs are done to the FIU, if the SMI has reasonable ground of believing that the transaction, including an attempted transaction, involves proceeds of crime, irrespective of the amount of the transaction. The SII should request for the statistics of such reports and if possible, a sample of the reports that have been submitted to the FIU. If the SMI cannot furnish the reports, the SII could request for such reports from the FIU to be rest assured that these submissions are being made. The SII should compare the date when the STR was submitted to the FIU versus the time when the suspicious transaction was realised. These reports are to have been submitted to the FIU within three days after determination that the transaction is suspicious.

The SII shall also verify if the SMI is submitting cash transaction reports (for those institutions that handle cash) to the FIU through requesting for such reports. Designated institutions are required to report every transaction conducted by or on behalf of a customer, equal to or exceeding $5,000, whether in one single transaction or in two or more transactions, totalling at least $5,000, conducted within a time period of 24 hours. It is required that these reports be submitted to the Unit on a monthly basis on or before the 10th of every month, of the preceding

month. If the SMI is a bank, then these reports should be submitted on a weekly basis, on or before the 2nd working day of the week.

Through interviews with the compliance personnel and staff members from the SMI, the SLO responsible for the inspection should verify if the procedures for suspicious transaction reporting are effective, through ensuring that employees who would have filed STR do not discuss their suspicions with anyone other than compliance employees within the SMI. The SII should also ensure that these suspicions are not discussed with the client as this would constitute tipping off.

The inspection should ensure that the SMI has sufficient controls in place to detect activities or transactions that are suspected to be related to terrorist property, and that these are reported to the FIU as and when they are realised. It is also important to ensure sufficient controls are in place to detect the presence of property controlled by the SMI on behalf of persons or entities that have been designated as terrorists by the United Nations Securities Council (UNSC) and that these situations are reported to the FIU.

The SII should ensure that appropriate measures are in place to prevent any funding, the provision of any financial or other service, or the provision of economic support directly or indirectly to any person or entity that is subject to financial sanctions issued by the UNSC. On that note, the SMI should be on the lookout for any directive issued by the FIU or the Securities and Exchange Commission on the sanctioned entities and individuals and must take action within 24 hours of receipt of such directive, should one of their clients be on the sanctions list.

Maintenance of records of Transactions

The SII should ensure that records of all client acceptances and verification documents are compiled and maintained for a minimum period of five years after

the termination of the relationship with the client, or in instances of a single transaction, that the records are kept for at least five years after the date of the single transaction. This also applies to records of transactions or activities that give rise to the filing of a suspicious transaction report.

Information maintained in respect of transactions permit reconstruction of individual transactions, and if necessary, evidence for prosecution of persons involved in criminal activity. The SII should ensure that the SMI retains all client identification information and data obtained through the CDD process (e.g. identification documents such as identity cards, passports, driving licenses, account files and relevant business correspondence). The SII should also check for the availability of records concerning AML/CFT training for the SMI as evidence of training undertaken.

The records may be kept in hard copy or electronic format and they must be stored securely against fire, water and systems damage. The SII should evaluate the appropriateness of steps adopted by the SMI to evolve and maintain a system that allows data to be retrieved easily and without delay whenever required or when requested by competent authorities.

Customer education and Employees Training

Financial institutions are required to design comprehensive employee education and training programs not only to make employees fully aware of their obligations, but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks. The establishment of such an employee training program is not only considered as best practice but a statutory requirement.

The SII should therefor ensure that the SMI conducts an ongoing employee training programme which ensures that members of staff are adequately trained so that they are aware of;

a) policies and procedures relating to prevention of money laundering and counter terrorist financing, and

b) the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of transactions.

It is crucial that all staff members responsible for combating ML and TF fully understand the rationale behind the AML/CFT policies, and the need for them to implement such policies consistently. The SII, through interviewing staff members of the SMI, should evaluate their level of knowledge and understanding of AML/CFT related matters and whether they are aware of the suspicious transactions reporting procedures. The SII should also evaluate the AML/CFT culture of the SMI through these interviews or through the use of AML questionnaires.

The SII should verify whether the SMIs review their AML/CFT framework from time to time with a view of determining their adequacy and identifying other areas of potential risks not covered by the AML/CFT Compliance Manual. The SMI should keep a record of all AML/CFT training materials delivered to its employees together with the statistics of how many have been trained and how many are yet to be trained. The SII should also find out the frequency of such training and evaluate its adequacy. A calendar of upcoming training should be available together with a list of which staff members will undergo the training.

Training can be face to face or can be conducted online. If training is conducted online, then the SII should evaluate the effectiveness of the measures taken by the SMI to ensure that every staff member has gone through that training and

clearly understands what the content of the training entails. For face to face training, information on the date of the training, the person who conducted the training and the attendees should also be available.

Other considerations

The SII must check if the SMI under inspection maintains the UNSC sanctions list register and that it is updated daily. The SII should also establish whether the SMI reverts to the FIU whenever the Unit issues a directive on any update on the sanction list even when the SMI has a nil return. The compliance person at the SMI should visit the UNSC website twice a day, in the morning and in the afternoon to check whether there are any updates on the sanctions list.

c) Working papers

Working papers should be prepared for every area reviewed during the inspection in order to document inspection procedures and support conclusions. They must provide sufficient documentation for a reviewer to understand what was done, why it was done, and how conclusions were reached. Objectives, findings, risks associated with deficiencies, conclusion and recommendations should be clearly outlined in working papers.

The working papers for each area should contain only essential information that supports conclusions, violations of law or regulations, or any applicable corrective actions. Working papers are the property of SECZ and should not be released to external parties without prior authorization.

d) Managing an inspection

Managing an inspection is as important as planning it. The level and sophistication of management methods and procedures varies depending on the activities to be performed and the size and nature of the SMI.

The SII has a responsibility to ensure that supervisory objectives are met, and activities are completed timely. To accomplish these goals, the SII must continually monitor the progress of the inspection and supervise, coordinate, and evaluate the work flow.

e) Correction

One of the key objectives in managing an inspection is to effect a correction process of identified deficiencies. Inspectors seek SMI management's commitment to correct significant deficiencies and verify that the SMI's corrective actions have been implemented successful and timely.

In correction, inspectors

- Solicit commitments from management to correct each significant deficiency.
- Review SMI-prepared action plans to resolve each significant deficiency, including the appropriateness of the time frames for correction.
- Verify that the SMI is executing the action plans.
- Evaluate whether the actions the SMI has taken (or plans to take) adequately address the deficiencies.
- Resolve open supervisory issues through informal or formal actions.

Inspectors should ensure that SMI management's efforts to correct deficiencies address *root causes* rather than symptoms. To do so, inspectors may require management to develop new systems or improve the design and implementation of existing systems or processes.

The SMI's plans for corrective actions should be formally communicated through action plans. Action plans detail steps or methods management has determined will correct the root causes of deficiencies. SMI management is responsible for developing and executing action plans. Directors are expected to hold management accountable for executing action plans.

Action plans should:

- Specify actions to correct deficiencies.
- Address the underlying root causes of significant deficiencies.
- Set realistic time frames for completion.
- Establish benchmarks to measure progress toward completion.
- Identify the SMI personnel who will be responsible for correction.
- Detail how the board and management will monitor actions and ensure effective execution of the plan.

The Commission's supervision of deficient areas focuses on verifying execution of the action plan and validating its success. When determining whether to take further action, inspectors consider the responsiveness of the SMI in recognizing the problem and formulating an effective solution. When the SMI is unresponsive or unable to effect resolution, the Commission may take more formal steps to ensure correction.

POST INSPECTION TIME LINE

Table 5: Post inspection timeline

DATE	ACTIVITY REQUIRED
Day 1	End of on-site Inspection
Day 15	Submission of provisional report to the Manager in Charge-SSD
Day -19	Onward submission of the provisional report to Head of SSD for review and approval
Day 22	Submit draft report to the board of directors of the SMI for comments
Day 29	Receive Comments from SMI
Day 30	Submission of the report to the CEO for consideration and approval
One day after approval by the CEO	Hold meetings with the SMI

f) Exit Meeting

After the conclusion of every on-site inspection, the inspection team shall hold an exit meeting with management to discuss inspection findings, conclusions, and recommendations based upon the ML/TF Risk Assessment of the SMI; discuss potential courses of action to address deficiencies.

The meeting will discuss the areas of greatest ML/TF risk to the SMI, preliminary ratings, and plans for future supervisory activities. The SII should encourage SMIs to respond to SECZ concerns, provide clarification, ask about future supervisory plans, and raise any other questions or concerns. At the exit meeting, the inspectors will ask for management's commitment to correct weaknesses noted during the supervisory activity.

Before the exit meeting, the SII should discuss significant findings, including preliminary ratings with the SECZ supervisory management. This discussion helps ensure that SECZ policy is consistently applied and that SECZ management supports the conclusions and any corrective actions deemed necessary. The SII and the supervisory office should also decide on who will attend the exit meeting on behalf of the Commission and inquire about the attendance of senior SMI managers and others.

Inspectors must ensure that any significant decisions discussed during the exit meeting are effectively conveyed in the meeting with the board and in written correspondence. Inspectors should discuss all issues with management before discussing them with the board, unless, in the supervisory office's view, the subject is best approached confidentially with the board.

g) Written Communication and meetings

Written communication of supervisory activities and findings is essential for effective supervision. Inspectors should periodically provide written

communication to the board highlighting significant issues that arise during the supervisory process. This communication should focus the board's attention on SECZ's major conclusions, including any significant problems. This written record, along with other related correspondence, helps establish and support the Commission's supervisory strategy.

Written communication must:

- Be consistent with the tone, findings, and conclusions orally communicated to the SMI.
- Be addressed to the appropriate audience based on how the SMI or company is structured and managed.
- Discuss any concerns the Commission has about SMI ML/TF risks, deficiencies in risk management, or significant violations.
- Summarize the actions and commitments that the Commission will require of the SMI to correct deficiencies and violations.
- Be concise to ensure that the issues are clear.

In addition to written communication throughout a supervisory cycle, **the Commission will provide each SMI's board of directors an Inspection Report (IR) at least once during every supervisory cycle.** The IR conveys the ML/TF risk profile of the SMI and summarizes inspection activities and findings during the supervisory cycle.

Meeting with the board of directors

The Commission maintains communication with boards of directors throughout the supervisory cycle to discuss SECZ inspection results and other matters of mutual interest, including current industry issues, emerging industry risks, and legislative issues. The SII will meet with the board of directors or an authorized committee that includes outside directors after the board or committee has

reviewed the report of inspection findings. If necessary, the Commission will use board meetings to discuss how the board plans to respond to supervisory concerns and issues.

The Commission will conduct a meeting with SMI board of directors at least once during every supervisory cycle for the SMI. More frequent meetings should be conducted when justified by the SMI's condition or special supervisory needs.

The SII on conducting the meeting should be prepared to discuss methods of corrective action, as well as to discuss all findings, conclusions, and concerns. The SII should encourage board members to ask questions or make comments. Senior management of the appropriate SECZ supervisory office should attend and participate in board meetings. If the inspection was conducted jointly with another regulator, the supervisory office should invite a representative from that agency to participate in the board meeting.

Meeting with Administrators and/or Custodians

The Commission will conduct a meeting with Administrators and or Custodians at least once during every supervisory cycle for the SMI. The Commission will discuss performance and misconduct issues of the SMI.

h) Inspection Report

An inspection report is the SMI's primary vehicle for communicating inspection findings in writing to the SMI's management and board of directors. The report should define the objectives and focus of the inspection, state its conclusions, and identify any significant problems, corrective action, and timeframes for corrective action.

The objectives of an Inspection report are:

a. to inform the board and management of the inspectors' assessment of ML/TF risks, and adequacy of risk management systems;

b. recommend to the SMI's management on the corrective measures and time frames; and

c. serve as a permanent record of evaluation of the ML/TF condition of an SMI to be used for future reference.

Supervisory ratings should be disclosed, and they should reflect the adequacy of the risk management systems/structures in light of the types and level of risks identified. The Inspection Report should contain both qualitative and quantitative factors.

The inspection report comprises three mutually reinforcing sections, namely: Background, Summary of Findings and Matters Requiring Attention, Core Assessment, and the Supplementary Sections.

The **Background** section provides the SMI Overview; Objectives and Scope of Inspection; and overall Condition;

The **Summary of Findings and Matters Requiring Attention** illustrates the conclusion of the report; AML issues that need attention; and Compliance issues.

The **Core Assessment** section consists of a detailed ML/TF Risk Management Review and assessment. The section starts with the Risk Management Review in order to underscore the primacy of ML/TF risk management and analyses each ML/TF risk category.

7.4.5. FOLLOW-UP AND MONITORING

The objective of this activity is to follow-up on implementation of the supervisory directives and recommendations made to the inspected SMI. The SII should

maintain an ongoing list of issues to be followed up with the SMI's management within a specified timeframe. The results may be incorporated in the SMI profile updates.

A range of tools are available to monitor the implementation of AML/CFT defences by SMIs. These include the use of periodic reporting, information from the FIU, the use of professionals, questionnaires and onsite inspections. The mechanisms are as detailed below.

a) Periodic reporting

The Commission should place an obligation on SMIs to make periodic AML/CFT reports on a quarterly basis in addition to the quarterly financial reports that they already submit. Categories of information that could be obtained from periodic reports can provide useful information on the state of compliance with AML/CFT obligations. The precise selection of the information to be required in periodic reports should be determined based on the SLO's assessment of the ML/TF risks in the Securities sector. Some examples of periodic reporting requirements are set out below:

- Risk assessment
- Customer acceptance policy and procedure
- Customers in different risk categories
- Complaints
- Number of PEPs
- Internal audit reports
- Compliance officer reports
- STRs received by the MLRO and not submitted to the FIU
- Training records and training needs analysis
- Analysis of refused business

Information on such matters as the risk assessment and various policies and procedures are analysed to determine, firstly, if the SMI has arrangements in place, and secondly, to judge their quality. Data on customers in risk categories, the breakdown of customers by location or business, complaints, and the number of politically exposed persons (PEPs) is helpful in judging the risks of the SMI, as well as determining if the SMI is, in fact, implementing the kind of management information system that would enable it to keep track of ML/TF risks, and the effectiveness of policies and procedures in mitigating such risks.

Reports issued by the internal auditor should also be submitted and should cover the extent to which the policies and procedures, as currently framed, are being implemented. The information in such reports can also be used to assess ML/TF risk, and to discuss risks with management at management meetings.

Information on the number of internal reports of suspicious transactions should be compared with the number of reports actually submitted to the FIU. If there are many internal reports and that only a few are reported to the FIU, then this could possibly imply that the SMI is wrongly holding back reports. While such data cannot be definitive on its own, it may prompt questions for the SLO to raise at meetings with management, or through an onsite inspection. Data on training, and information on the method of identifying training needs, will give information on the quality of AML/CFT training.

Where an SMI refuses to accept a customer, on the grounds of unacceptable ML or TF risk, such data can provide an indication of how seriously the SMI is conducting its risk assessment of customers. The periodic reports are the most comprehensive set of regular data obtained about SMIs, and it is important that it is used to adjust the risk scoring of each SMI according to the Commission's methodology.

b) Information from the FIU

The FIU receives suspicious transaction reports and is responsible for investigating the reports and following up on any allegations of ML or TF. The Unit can provide information on the effectiveness of reports filed by SMIs and can also furnish information on the adequacy of the record-keeping by SMIs as evidenced by their ability to supply information and trace funds. This information is valuable and reflects the state of compliance by SMIs with their AML/CFT obligations.

c) Themed third-party reviews and questionnaires

The Commission can also appoint third parties (such as audit or law firms) to carry out specific investigations. This is particularly useful when there is a need to review the state of compliance with a particular aspect of the AML/CFT defences, such as the measures that detect whether customers are PEPs, or the measures that identify beneficial owners. Such themed reviews by third parties, if properly commissioned, can provide useful intelligence.

Similarly, The SLO can conduct a survey of the SMI through the use of a well-structured questionnaire to establish compliance with a particular aspect of the AML/CFT obligations. This can be used to obtain data, when it is not supplied routinely through periodic reports.

d) Onsite Inspections

Onsite inspections remain a vital part of the supervisor's tool kit. Inspections can take the form of a full-scope inspection, designed to determine the level of compliance with all aspects of the AML/CFT regime; they can also be themed, to establish the level of compliance with a particular aspect of the regime, by all, or several SMIs; or they can be targeted, to review a specific aspect of compliance by a specific SMI, or any combination of these.

The SLOs can conduct inspections without cause or notice, although it is usually more efficient to give notice. The inspection programme should be determined on the basis of the risk assessment of the SLO, and the selection methodology should take account of the time since the last inspection, so that even the lowest risk licensees are inspected at some stage. As a general principle, no SMI that is subject to routine inspections should have a gap of more than four years between inspections.

Each inspection should be carefully planned by consulting the information from periodic reports and previous inspections so as to define a set of objectives and issues that are specific to the inspected SMI. It is not sufficient to rely on generic objectives, as this does not make maximum use of supervisory intelligence. The objectives and issues should determine the approach and methodology of the inspection.

The SMI to be inspected should be informed of which documents and files should be made available before and during the inspection, although some files should be demanded without notice, so as to test the SMI's readiness. The precise scope of an inspection should depend on the risk assessment and risk scoring, but the SLO can also focus, at least in part, on the governance of the SMI. This will require an examination of papers submitted to senior management and the board of directors. Minutes of senior management's and risk committees' meetings should be reviewed, and interviews held with senior management.

The SLO should test the quality of the risk assessment, the nature of the policies and procedures, particularly customer acceptance policy and due diligence procedures, customer monitoring and review, reporting, training, controls, and staff screening. The conclusions of the inspection should be communicated to the SMI, a draft report submitted in reasonable time, and an action plan agreed with the SMI with timetables and a reporting procedure.

8. PENALTIES FRAMEWORK

The Commission is empowered to impose penalties by the Financial Intelligence Unit's **AML/CFT Directive 2/2014** within the scope of **Section 5 of the MLPC Act Chapter (9:24)**. Further, the Commission has additional powers to impose penalties in terms of **Section 105 of the Securities and Exchange Act Chapter (24:25).**

9. APPENDICES

Appendix 1: Examples of information relating to Institutional Profile

Key aspects of institution	Examples of information to include and possible AML/CFT risk sources
History of institution	– Determine date established, obtain and name changes – Describe history of the institution with specific reference to AML/CFT.
Vision, mission, strategy	– Outline key AML/CFT considerations associated with the institution's vision, mission, and strategy. – Describe AML/CFT implications and identify ML/TF risk appetite – Describe AML/CFT compliance culture.
Group structure	– Obtain group organogramme. – Identify major shareholders (e.g. owning 10% or more). – Describe the group structure and identify mergers, acquisitions and disposals.
Organisation size and nature	– Establish the organization size and nature. – Note AML/CFT implications.
Board of directors	– Obtain names of the board of directors. – Identify board of directors' knowledge, skills, and experience relating to AML/CFT. – Identify information that reflects on the integrity of board of directors. – Identify additional business and other relationships the board of directors' members may have. – Check if board members are not Politically Exposed Persons (PEPs)

Board and management committees	– Identity board and management committees and determine their roles and responsibilities relating to AML/CFT.
Staff compliment	– Describe management and staff knowledge, skills and experience relating to AML/CFT.
Business model	– Describe the institution's business model. – Note ML/TF implications.
Lines of business	– Describe the institution's lines of business. – Note ML/TF implications.
Products and services	– Describe the products and services of the institution. – Note ML/TF risks relating to the products and services.
Risk management function	– Describe the risk management framework and process of the institution. – Note AML/CFT considerations. – Adequacy and effectiveness of the risk management framework and process.
Compliance function	– Describe the compliance framework and process of the institution. – Note AML/CFT considerations. – Adequacy and effectiveness of the compliance framework and process.

Diana Madondo----------Date---------
Supervision and Licensing Officer

Laurencia Mukuwe----------Date----------
Supervision and Licensing Officer

Bethwell Purazeni----------Date----------
Supervision and Licensing Officer

Tirivafi Nhundu----------Date----------
Manager: Supervision and Licensing

Norman Maferefa----------Date----------
Head: Supervision and Surveillance