Financial Intelligence Centre

PUBLIC COMPLIANCE COMMUNICATION

PUBLIC COMPLIANCE COMMUNICATION No 53

ON THE RISK MANAGEMENT AND COMPLIANCE PROGRAMME IN TERMS OF SECTION 42 OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT 38 OF 2001) FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

PCC SUMMARY

This public compliance communication 53 (PCC 53) provides guidance to accountable institutions that are designated non-financial businesses and professions (DNFBPs), on the drafting of a risk management and compliance programme (RMCP) document describing the RMCP, in line with section 42 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act).

PCC 53 is limited to assisting DNFBP accountable institutions better understand how to approach money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risk assessment, identification, mitigation, management and monitoring within their businesses.

This PCC 53 is intended for DNFBP accountable institutions. PCC 53 is not intended for financial institutions, DNFBPs that fall within group structures, and DNFBPs that have advanced compliance or complex structures.

THE AUTHORITATIVE NATURE OF GUIDANCE

The Financial Intelligence Centre (Centre) provides the guidance contained in this PCC in terms of its statutory function in terms of section 4(c) of the FIC Act read together with Regulation 28 of the Money Laundering and Terrorist Financing Control Regulations (Regulations) issued in terms of the FIC Act.

Section 4 (c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations in terms of the FIC Act. Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Regulations issued in terms of the FIC Act. Accordingly, guidance provided by the Centre is authoritative in nature and must be considered when interpreting the provisions of the FIC Act or assessing compliance of an accountable or reporting institution with the obligations imposed on it by the FIC Act.

It is important to note that enforcement action may emanate as a result of non-compliance with the FIC Act in areas where there has been non-compliance with the guidance provided

by the Centre. Where it is found that an accountable or reporting institution has not followed guidance which the Centre has issued, the institution must be able to demonstrate that it has complied with the relevant obligation under the FIC Act in an equivalent manner nonetheless.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the users' legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

OBJECTIVE

The objective of this PCC 53 is to provide guidance to DNFBPs on the development of an RMCP document that describes the RMCP as required in terms of section 42 of the FIC Act.

1. Introduction

1.1. Accountable institutions must develop, document, maintain and implement a risk management and compliance programme (RMCP) for anti-money laundering , and combating the financing of terrorism (AML/CTF). The RMCP must provide for all the requirements as set out in section 42 of the FIC Act. In addition, the Centre strongly encourages accountable institutions to identify, assess, monitor, mitigate and manage the risk of proliferation financing (PF), and include counter proliferation financing risk (CPF) mitigation measures in the RMCP.

1.2. The Centre recommends that accountable institutions that are designated non-financial businesses and professions (DNFBPs) describe their RMCP in a consolidated document, which is referred to as the RMCP document.

1.3. A DNFBP accountable institution must express and include the money laundering, and terrorist financing (ML/TF) risks, and its understanding flowing from the risk assessments, and the risk mitigation, monitoring as well as the management measures in the RMCP document.

1.4. A DNFBP accountable institution should note that in response to a request for documentation in terms of section 42(4) of the FIC Act, the accountable institution should provide the RMCP document. Failure to produce an RMCP document to the supervisory body or the Centre would amount to non-compliance.

1.5. A DNFBP accountable institution must make its RMCP document available to each of its employees.

1.6. PCC 53 is intended for DNFBP accountable institutions (such as trust service providers) that do not form part of group structures and do not have advanced compliance or complex structures. This PCC 53 is not intended for financial institutions and larger accountable institutions that have advanced compliance or complex structures, including DNFBP accountable institutions within those structures.

1.7. Financial institutions and larger accountable institutions generally have more complex business models. As a result, this simplified guidance and associated template may not be as effective, although the principles contained may be applied and expanded upon.

1.8. The accountable institution's RMCP document must provide for all the requirements as set out in section 42 read with section 42A of the FIC Act and are discussed thematically as follows:

1.8.1. The RMCP governance
1.8.2. ML/TF/PF risks assessment and risk-rating framework
1.8.3. Customer due diligence controls
1.8.4. Targeted financial sanctions controls aimed at terrorist financing
1.8.5. Targeted financial sanctions controls aimed at proliferation financing (section 26A, 26B and 26C of the FIC Act)
1.8.6. Prominent influential person controls
1.8.7. Account monitoring
1.8.8. Reporting controls, and
1.8.9. Record-keeping controls.

1.9. This PCC includes a principal discussion of effective documentation of an RMCP document, a reference table of all applicable sections of the FIC Act that must be included in an RMCP (Annexure A), an editable template that could be used as a guide (Annexure B), and a list of indicators that may be used to assess the ML/TF/PF risk.

1.10. Accountable institutions are advised that the principles as set out in the FIC Guidance Note 7 and any future updates to Guidance Note 7 applies to all accountable institutions including the DNFBP accountable institutions for which this PCC is intended.

2. RMCP governance

2. An accountable institution should document the RMCP governance controls in the RMCP document, which must indicate:

2.1. The roles, responsibilities, governance structures and oversight functions of the section 42A compliance officer, the compliance function, board of directors, senior management or other persons exercising the highest level of authority in relation to compliance with the FIC Act and the accountable institution's RMCP.

2.2. The accountable institution must appoint a compliance officer and be able to demonstrate that this person has sufficient competence and seniority. This can be done by naming who the section 42A compliance officer is, and the level of competence and seniority that person holds.

2.3. Documented approval of the RMCP by board of directors, senior management or other persons exercising the highest level of authority.

2.4. The regular interval dates upon when the RMCP will be reviewed. The Centre recommends that the accountable institution reviews its RMCP annually, as ML/TF/PF risks change continuously.

2.5. The process to implement the RMCP and its dissemination to employees. The accountable institution could implement its RMCP through various controls which include, but are not limited to their policies, processes, systems, employees, and training.

2.6. The AML/CFT/CPF training controls that apply within the accountable institution.

2.7. The requirement to escalate AML/CFT/CPF breaches in control measures to board of directors, senior management or other persons exercising the highest level of authority.

2.8. The high-level remediation processes accountable institutions must implement based upon the different AML/CFT/CPF breaches.

3. ML/TF/PF risk assessment and risk-rating framework

3.1. Refer to Chapter 1 of the Centre's Guidance Note 7, which discusses the principles that apply for the adoption of a risk-based approach. An accountable institution must include the manner in which it **identifies, assesses, monitors, mitigates and manages** the ML/TF/PF risk. This also includes the manner in which the accountable institutions rates the level of ML/TF/PF risks. The ML/TF/PF risk assessment and identification forms the basis of the accountable institution's RMCP, and the accountable institution must therefore be able to demonstrate the risk assessment and identification as a first step in the development of an RMCP.

3.2. This risk-based approach must provide for:

3.2.1. A **business-level risk assessment** indicating the ML/TF/PF risk the accountable institution as an entity faces, and the risk each of the accountable institution's different business areas faces.

3.2.2. The manner in which the accountable institution would assess **new products and services** to determine the ML/TF/PF risk ratings or weightings.

3.2.3. A **client-level** risk assessment indicating the ML/TF/PF risks different business relationships or single transactions pose. Annexure C sets out some of the indicators as highlighted in FIC Guidance Note 7, which broadly includes client type, delivery channel, geographic location (e.g. countries/regions/areas/towns etc.), products and services as well as any other relevant factors.

3.2.4. The accountable institution must stipulate which indicators should be considered when conducting the risk assessments. The accountable institution is advised to consider the indicators holistically.

3.2.5. The accountable institution must demonstrate that it has conducted client-level risk assessments before establishing a business relationship or concluding single transactions with each client, and periodically thereafter as risk changes.

3.2.6. The accountable institution must demonstrate that it has conducted a **business-level risk assessment**, as well as a risk assessment of **new products and services**.

3.2.7. A **client-level risk matrix** could serve as a tool to provide an objective basis for the assessment of several risk indicators in relation to a business relationship or single transaction with a client. The RMCP must provide for the manner in which the accountable institution risk rates or weighs the various indicators characteristics and the method of determining the overall risk ratings or weightings. The method may be a manual or automated manner of calculating ML/TF/PF risk ratings. Refer to Table 1 below as an example.

Table 1 example: Calculation of overall ML/TF/PF risk rating

Indicator	**Characteristic**	**Accountable institutions assessment of the ML/TF/PF risks**	**Risk-rating score** 1 – low 2 – medium 3 – high
Client	Insert client characteristic (e.g. nature of the client's business activity involves transacting in large amounts of cash)	Insert accountable institution's rational (e.g. deemed to present a higher ML/TF risk based upon historical trends, cash allows for anonymous transactions)	Insert proposed scoring (e.g. 3)
Client	Insert client characteristic (e.g. complex corporate structure)	Considering various guidance, including FATF guidance. Noting the risk of not understanding the beneficial owner, therefore complex structures present a greater ML/TF/PF risk.	Insert proposed scoring (e.g., 3)
Client	Insert client characteristic (e.g. foreign	Insert accountable institution's rational (e.g. perceived higher susceptibility to corruption –	Insert proposed scoring (e.g., 3)

	prominent public official	trends and typologies identified by the FATF). Trends indicate a higher likelihood of ML/TF.	
Product or service	Insert product/service characteristic (e.g. product that allows for cash payment, or third-party payment)	Insert accountable institution's rational (e.g. where cash is used, trends indicate higher likelihood of criminals using proceeds of crime to buy immovable property – therefore heightened risk). Therefore, overall deemed medium risk.	Insert proposed scoring (e.g. 2)
Product or service	Insert product/service characteristic (e.g. the product provide anonymity to the client - creating a trust)	Insert accountable institution's rational (e.g. considering various guidance, including FATF guidance). Noting the risk of not understanding the beneficial owner, therefore complex structures present a greater ML/TF/PF risk.	Insert proposed scoring (e.g. 3)
Geographic location (domestic and international)	Insert geographic area characteristic (e.g. country/ province/town)	Insert accountable institution's rational (e.g. geographic area has been identified by credible sources as a high-risk area.)	Insert proposed scoring (e.g. 3)
Geographic location	Insert geographic area characteristic (e.g. a country which is the subject of a sanctions regime)	Insert accountable institution's rational (e.g. North Korea is subject to UNSC sanctions, therefore presents a PF risk)	Insert proposed scoring (e.g. 3)
Delivery channel	Insert delivery channel characteristic (e.g. non face to face)	Insert accountable institution's rational (e.g. higher risk due to level of anonymity)	Insert proposed scoring (e.g. 3)
Other factors		Any other factor the accountable institution deems relevant	Insert proposed scoring (e.g. 3)
Total out of 5 indicators e.g. 15			Overall total of 5 factors combined equal's total.
Combined total of risk rating/weight (sum of 5 indicators rating combined)		**Risk allocation**	**Level of CDD required**
e.g. 1 to 5		e.g. Low risk	e.g. Simplified due diligence

e.g. 6 to 10	e.g, Medium risk	e.g. Standard CDD
e.g. 11 to 15	e.g. High risk	e.g. Enhanced due diligence
List automatic high-risk e.g. client FPPO etc.		
List automatic high-risk do not proceed to establish business relationship or conduct single transaction e.g. person is listed on a Targeted Financial Sanctions list etc.		

3.2.8. The risk-based approach framework should set out the intervals at which the risk rating will be determined including at the establishment of a new business relationship, before conducting a single transaction and thereafter at pre-determined ongoing due diligence intervals.

3.2.9. The actual risk rating or weighting assigned to each factor's characteristic should be recorded as part of the methodology and applied uniformly when risk rating.

3.2.10. The manner in which to record the outcome or /results of the risk assessments that are conducted (e.g. when a client establishes a business relationship the outcome risk rating is recorded on the client file).

3.3. The accountable institution can make an informed decision as to the appropriate methods and levels of verification and enhanced controls that must be applied in a given circumstance on the basis of risk assessment results.

3.4. The **monitoring, mitigating and management controls** that must be applied to the different risk ratings must be clearly noted. The steps that must be taken after having assessed the risks must be indicated.

3.5. The RMCP document must provide for the documenting of **decisions taken** when dealing with the different levels of ML/TF/PF risks.

4. Customer due diligence controls

4. The accountable institution must include in the RMCP document its customer due diligence (CDD) processes, which should indicate the manner in which the accountable institution:

4.1. Determines which persons are deemed to be clients, and further determine whether a person(s) is an existing client.

4.2. Prevents the on-boarding of anonymous clients, and clients acting under a false or fictitious name.

4.3. Conducts CDD on the different types of prospective clients, existing clients, beneficial owners, persons acting on behalf of the client and other persons. This includes determining the level of verification which forms part of the CDD as a result of the client's risk rating.

4.4. Conducts additional due diligence (ADD) in respect of clients that are legal persons, trusts or partnerships.

4.5. Conducts ongoing due diligence (ODD) and at which intervals.

4.6. Conducts enhanced due diligence (EDD) where a high-risk business relationship or single transaction has been identified.

4.7. Conducts simplified due diligence where a low-risk business relationship or single transactions has been identified.

4.8. Conducts client on-boarding approval including for high-risk business relationships or single transactions.

4.9. Determines processes where CDD cannot be conducted, including where the accountable institution must not enter into business relationship or conduct a single transaction, and where an existing business relationship should be

terminated and consider filing a suspicious transaction report (refer to section 21E of the FIC Act).

4.10. Conducts client profiling including determining which future transactions are consistent with the accountable institution's knowledge of a prospective client.

4.11. Confirms information relating to a client, where the accountable institution doubts the accuracy of previously obtained information.

4.12. May conduct CDD where there is a suspicion regarding a once-off transaction that is less than R5000.00.

5. Targeted financial sanctions controls relating to terrorist financing

5. The accountable institution must detail the process to comply with the targeted financial sanctions regime aimed at terrorist financing in the RMCP document (refer to PCC 44). A targeted financial sanctions (TFS) process must provide for:

5.1. The manner in which the accountable institution will scrutinise client information in order to identify persons listed on a United Nations Security Council 1267 resolutions list, that is published in terms of section 25 of the Protection of Constitutional Democracy Against Terrorism and Related Activity Act, 2004 (Act 33 of 2004) (POCDATARA Act).

5.2. The systems used and supporting processes for scrutinising client information.

5.3. The freezing of accounts process that must be followed should a client or potential client be listed on a TFS list.

5.4. It is important to note that client information includes information regarding the client, the prospective client, beneficial owner, person acting on behalf of the client and transaction/payment information.

6. Targeted financial sanctions controls relating to proliferation financing

6. The accountable institution should document its processes in place to comply with the TFS regime aimed at proliferation financing, as set out in section 26A, 26B and 26C of the FIC Act in the RMCP document (refer to PCC 44). A TFS process must provide for:

6.1. The manner in which the accountable institution will scrutinise client information in order to identify persons listed on a TFS list as published on the Centre's website in terms of section 26A of the FIC Act.

6.2. The systems used and supporting processes for scrutinising client information.

6.3. The freezing process that must be followed should a client or potential client be listed on a TFS list.

6.4. It is important to note that client information includes information regarding the client, prospective client, beneficial owner, person acting on behalf of the client and transaction or payment information.

7. Prominent influential persons controls

7. An accountable institution must document its process regarding prominent influential persons in the RMCP document which sets out:

7.1. The manner in which the accountable institution scrutinises prospective clients, persons acting on behalf of the client and the beneficial owner's information to determine whether they are domestic prominent influential persons (DPIP) foreign prominent public officials (FPPO), their immediate family members or known close associates (refer to PCC 51).

7.2. The manner in which the accountable institution will obtain senior management approval to establish a business relationship with an FPPO, or if considered high-risk, a DPIP.

7.3. The manner in which the accountable institution will determine the source of funds and wealth of a client that is an FPPO, a high-risk DPIP, their immediate family member or known close associate.

7.4. The data sources relied upon to determine whether a client is an FPPO or DPIP.

8. Account transaction or activity monitoring

8. An accountable institution must include its process to monitor client transactional activity in the RMCP document, which indicates:

8.1. The manual or automated processes in place for account, transaction or activity monitoring in terms of section 21C of the FIC Act, to determine whether the transactions or activity is consistent with the client's business and risk profile.

8.2. The manner in which accountable institution will examine complex and unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose, as well as the process in place to keep written findings of the accountable institution's decisions in this regard.

9. Reporting controls

9. The accountable institution must document its reporting process in the RMCP document which sets out:

9.1. The end-to-end internal process for identifying possible reportable transactions (refer also to Directive 5 and PCC 45), analyse and report transactions to the Centre, in terms of sections 28, section 28A, and section 29, where applicable. This would include who must submit the report, and the periods within which the reports must be submitted to the Centre.

9.2. The process in place to keep written findings of the accountable institution's decisions to report or not.

9.3. The process in place to deal with section 27, section 32, section 34 requests and section 35 monitoring orders in terms of the FIC Act.

9.4. A clear instruction on tipping off and the non-disclosure of suspicious transaction reports (STRs) to other persons (see PCC 42).

10. Record-keeping controls

10. An accountable institution must document its record-keeping process in the RMCP document. It is the Centre's view that this process should clearly indicate records access and confidentiality controls. This process could include:

10.1. What records must be kept

10.2. In what format will these records be kept (e.g. hard copies or electronic records)

10.3. The period for which records must be kept

10.4. If the records are kept by a third party, details thereof as prescribed in regulation 20 of the Money Laundering and Terrorist Financing Control Regulations.

11. COMMUNICATION WITH THE CENTRE

11.1. The Centre has a dedicated compliance contact centre geared to assist accountable institutions to understand their registration obligations in terms of the FIC Act. Please call the compliance contact centre on 012 641 6000 and select option 1.

11.2. Compliance queries may also be submitted online by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx or visiting the Centre's website and submitting an online compliance query.

Issued by:

The Director

Financial Intelligence Centre

30 August 2022

Annexure A: Section 42 of the FIC Act – reference table

Topic/obligation	Section	Issues that must be addressed	Guidance
RMCP governance	42(2)q	Ensure that the RMCP is implemented in branches, subsidiaries or other operations of the institution including in foreign countries. If the institution does not have any branches, then it must indicate in its RMCP that section 42(2)(q) of the FIC Act is not applicable.	Guidance Note 7
	42(2)r	Explain how the RMCP is going to be implemented	
	42(2B)	The documented approval of the RMCP by the board of directors, senior management or the person exercising the highest level of authority in an accountable institution.	
	42(2C)	Detail when the RMCP must be reviewed, and keep evidence to track the review and/or updates	
	42(3)	Make the RMCP available to employees	
	42(4)	Detail how to send a copy of the RMCP to the FIC or the supervisory body when required.	
	42(s) and 42A	Assign a compliance officer responsible for ensuring the effectiveness of the institution's compliance function, who is knowledgeable of the FIC Act and the institution's RMCP and with sufficient seniority to ensure compliance with the FIC Act and the institution's RMCP.	

Training	42(s) and 43	Determine how often training on the FIC Act and the institution's RMCP will take place, in what format and who must attend.	Guidance Note 7

Topic/obligation	Section	Issues that must be addressed	Guidance
Risk identification	42(2)a	Identify, assess, monitor, mitigate and manage risk of ML and TF	Guidance Note 7

Topic/obligation	Section	Issues that must be addressed	Guidance
CDD controls	42(2)b	Determination of prospective client and client that has established a business relationship or entering into a single transaction with the institution	Guidance Note 7 PCC22 PCC30 PCC31
	42(2)c	Ensure there are no anonymous clients	Guidance Note 7
	42(2)d and m	What information and documentation would be required per ML/TF risk rating for natural persons, legal entities, trusts and partnerships. Specify the CDD required for higher risk versus lower risk clients	Guidance Note 7
	42(e)	Understanding and obtaining information on a business relationship by providing for the manner in which the institution will determine whether future transactions that will be performed in the course of the business relationship are consistent with	Guidance Note 7

		the institution's knowledge of a prospective client.	
	42(2)f	Provide for the manner in which and the processes by which the institution conducts additional due diligence measures in respect of legal persons, trusts and partnerships to establish the nature of the client's business and the ownership and control structure of the client	Guidance Note 7
	42(2)g	Provide for the manner in which and the processes by which ongoing due diligence and account monitoring in respect of business relationships is conducted by the institution	Guidance Note 7
	42(h)	Provide for the manner to examine (i) complex or unusually large transactions and (ii) unusual patterns of transactions which have no apparent business or lawful purpose and keeping of written findings relating thereto.	Guidance Note 7
	42(2)i	Determine how to verify and confirm client information where there is doubt about information previously obtained	Guidance Note 7
	42(2)j	CDD considerations when there is a suspicious or unusual activity or transaction detected	Guidance Note 7
	42(2)k	Determine when/how a relationship will be terminated where CDD is not obtained	Guidance Note 7

Prominent influential persons

Topic/obligation	Section	Issues that must be addressed	Guidance
Prominent influential persons controls	42(2)l	How to determine if a client is a DPIP or FPPO	Guidance Note 7 PCC 51

Targeted financial sanctions

Topic/obligation	Section	Issues that must be addressed	Guidance
Targeted financial sanctions controls	42(2)s	What information will be scrutinised, and against which lists to determine if a client is a sanctioned person e.g. UN 1267 sanctions list and the TFS list	Guidance Note 6A Guidance Note 7 PCC 44

Account monitoring and reporting

Topic / obligation	Section	Issues that must be addressed	Guidance
Account monitoring	42(2)e	What information to be obtained to determine client profile, and how to detect if the behaviour or transactions change (i.e. do not stay consistent)	Guidance Note 7
	42(2)g	Determine how accounts will be monitored in respect of a business relationship. Determine what ongoing due diligence is required	
	42(2)h	Determine how to examine complex or unusually large transactions and unusual transaction patters	

Reporting	42(2)o	Determine when transactions or activities are reportable to the Centre	Guidance Note 4B, 5B and 6A
	42(2)p	Detail the process for how to report to the Centre: include STRs, CTRs and TPRs	Guidance Note 4B, 5B and 6A

Record-keeping

Topic/obligation	Section	Issues that must be addressed	Guidance
Record-keeping	42(2)n and Regulation 20	Specify record-keeping for CDD, transactions and reports submitted to the Centre Detail what must be kept, where it is to be kept, how long it will be kept (e.g. 5 years) and in what format it will be kept. Is a third party keeping the records? And if so, how and when to notify and provide the Centre with the details of the third party	Guidance Note 7

Annexure B: Example of an RMCP document template for DNFBPs

IMPORTANT TO NOTE

Annexure B provides a proposed template framework, which accountable institutions that are specifically DNFBPs as stated in paragraph 1.4 above must customise and enhance to suite the ML/TF/PF risk unique to the accountable institution's business.

It is vital to understand that Annexure B does not provide a ready-to-use RMCP, but merely a basic framework from which accountable institutions can build. The Centre **strongly cautions** against accountable institutions copying this document as is without changes.

Where an accountable institution has not customised the RMCP template, that accountable institution would be non-compliant with the FIC Act obligations as it would not be able to demonstrate that it has adequately identified, assessed, monitored, mitigated or managed their ML/TF/PF risks.

A reminder that an RMCP is a programme that consist of various controls that must be implemented and that needs to be documented. The template below can assist in how to describe a programme, and also serves to guide accountable institutions as to what their RMCP document should consist of.

Insert title i.e. RISK MANAGEMENT AND COMPLIANCE PROGRAMME FOR (insert accountable institution DNFBP name e.g., XYZ)

(DATE)

RMCP governance

1.1. The directors or senior management of XYZ include:

a. Y with the following role and responsibilities _____ (*e.g. review and approval of RMCP*)

b. Z _____ (*e.g. review and approval of RMCP*)

Compliance function

1.2. The compliance function at XYZ comprises:

1.2.1. Mr A with the following role and responsibilities _____ (*e.g. head of compliance function, drafting of RMCP and approval of all high-risk clients*).

1.2.2. Mrs B with the following role and responsibilities _____ (*e.g. acts as the money laundering reporting officer (MLRO) and reports to the Centre on goAML*)

1.2.3. Ms C with the following role and responsibilities _____ (*e.g. the CDD consultant who will collect all FIC Act related documentation and information and will update on the client profile. Will report all suspicions to Mr A*)

1.3. All staff at XYZ will be required to comply with this RMCP and report all suspicious behaviour to Mr A.

1.4. XYZ assigns Mr A (*insert position title*), in terms of section 42A of the FIC Act, to ensure the effectiveness of the compliance function and compliance with the accountable institution's RMCP.

1.5. Mr A holds the following qualifications and experience _____ (*insert qualifications and experience. Demonstrate sufficient competence and seniority*)

RMCP approval

1.6. The RMCP has been approved by:

a. Mr Y (*insert position title*) date and signature; and

b. Mr Z (*insert position title*) date and signature.

RMCP review

1.7. The RMCP will be reviewed and updated:

1.7.1. At regular intervals at minimum (e.g. annually).

1.7.2. Where there is a material change to any process, within X months of this change being made (_____ *other examples: on a regular basis, insert interval, e.g., annually, every six months etc.)*

1.7.3. Where there is a legislative change to relevant legislation, within X (_____ *insert period e.g., months/days/weeks etc*) of this change being made.

Applicability

1.8. The RMCP applies to all employees and branches including foreign subsidiaries (*indicate various branches where applicable*) of XYZ and is made available via the following distribution channels: (*insert channels, e-mail, intranet, physical delivery etc*.) to the employees and various branches of the accountable institution.

Branch application (applicable where accountable institution has branches)

1.9. The RMCP will be implemented in the following manner in the branches, subsidiaries, and other operations of the accountable institution _____.

1.10. (*If there are no branches to record*) XYZ does not have any branches and therefore section 42(2)(q) is not applicable.

1.11. (*Where applicable*) The requirements as set out in the FIC Act is implementable in a foreign branch or subsidiary

1.12. The following requirements in terms of section 42 of the FIC Act____ are not applicable in the foreign branch due to the following reasons____ (*insert reasons*).

Training

1.13. The following anti-money laundering, counter terrorist financing and counter proliferation financing (AML/CTF/CPF) training will be provided to all employees of XYZ:

1.13.1. (*Insert various levels of training, e.g. starter training, intermediate, advanced*)

1.13.2. At the following intervals (*state the intervals, e.g. on induction of new employees, annually or every six months etc. for all employees*) on an ongoing basis.

1.13.3. Training will be facilitated by (*insert employee role*) and employees will be subject to an assessment after the training.

1.13.4. Evidence of training will be retained in the following manner _____. (*training registers must be held, as well as presentations, and confirmation of attendance at FIC events etc.)*

Escalation of non-compliance with RMCP or FIC Act

1.14. All instance of non-compliance with XYZ's RMCP or the FIC Act must be escalated to the ____ (*insert person/s i.e. directors, senior management/other persons exercising the highest level of authority*) immediately upon becoming aware thereof.

1.15. The following escalation of non-compliance process must be followed ____ (*insert process e.g. completion of a breach form, submission to compliance officer via e-mail etc*.)

1.16. The following corrective measures must be adhered to ___ (*insert corrective actions*).

Risk-based Approach

2.1. XYZs products include: (*list all products*)

2.1.1. (*e.g. product 1)*

2.1.2. (*e.g. product 2)*

2.2. XYZs services include: (*list all services*)

2.2.1. (*e.g. service 1)*

2.2.2. (*e.g. service 2)*

2.3. In terms of XYZ risk-based approach, XYZ will identify, assess, monitor, mitigate and manage the risks that the products and services offered may involve or facilitate money laundering activities, terrorist financing, or proliferation financing and related activities in the following manner: _____ (*Insert all the control measures e.g. risk assessment and identification of the risks the accountable institution as an entity faces, as well as the different business areas, products and services at product development stages, the risk assessment and identification of risks at a client level when client on-boarding and thereafter at ongoing due diligence points. The mitigation and management controls based upon the varying levels of risk. As well as conducting monitoring to determine levels of compliance with the RMCP. All controls must be proportionate to the ML/TF/PF risks*).

2.4. XYZ will identify risk and assess the ML/TF/PF risks at a business level, a new products and services level, and a client level by assessing following indicators (*insert the various indicators factors, refer to FIC Guidance Note 7 for a list of some indicators*).

2.5. The assessment of ML/TF/PF risks is done when establishing a business relationship, conducting a single transaction, and at ongoing due diligence stages.

2.6. The following activities are considered to be business relationships: _____ (*accountable institution must state what all activities that are business relationships*). Where a client transacts on a recurring basis, that client has entered a business

relationship with the XYZ regardless of the amount of the transaction. XYZ must conduct customer due diligence on the client (*refer to Guidance Note 7*).

2.7. The following activities are considered to be single transactions less than R5 000.: _____ (*accountable institution must state the types of transactions less than R5 000 for the purposes of section 20A of the FIC Act*). XYZ must obtain and record information for the client (refer to Guidance Note 7).

2.8. The following activities are considered to be single transactions above the R5 000: _____ (*accountable institution must state what is considered to be a single transaction of more than R5 000*). XYZ must conduct customer due diligence on the client (refer to Guidance Note 7).

2.9. XYZ determines the overall ML/TF/PF risk weightings/ratings a business relationship poses in the following manner _____ (*indicate method used e.g. manually or through an automated tool etc. indicate tool used if applicable e.g. excel risk matrix etc.*)

2.10. The outcome of the risk assessment impacts the level of the customer due diligence conducted, including what information and documentation is required for verification. Where the ML/TF/PF risk is:

2.10.1. Low – simplified due diligence must be conducted

2.10.2. Medium – standard customer due diligence must be conducted

2.10.3. High – enhanced due diligence must be conducted.

2.11. XYZ will not establish a business relationship with or conduct a single transaction in instances where _____ *(insert various instances e.g. insert where the client is linked to a listed terrorist, the client has numerous money laundering convictions/charges pending etc.*) as XYZ has determined the ML/TF/PF risk is not acceptable in such instances. XYZ has taken this decision due to the following considerations at minimum _____ (*insert rationale*)

2.12. The following instances require approval to be obtained from senior management in conjunction with the compliance officer before accepting a client and establishing a business relationship or concluding a single transaction where

_____

(*insert various instances e.g. the client is high-risk or FPPO/high-risk DPIP or their family members and known close associates or any deviation from approved documentation or risk assessment*).

2.13. The ratings table below is to be used in all instances for client risk rating: (*insert table of choice*)

2.14. XYZ determines risk with reference to the following factors (*insert all factors*), each factor is reviewed against the unique characteristic and risk consideration, thereafter, assigned a risk-rating score of either_____ (*insert scoring e.g. 1 which indicates low risk, 2 for medium risk and 3 for high risk*).

2.15. Dependent on the combined risk rating of all the scores assigned to the factors, XYZ will determine the level of due diligence to be applied, as indicated below

_____

(insert table showing risk ratings and corresponding level of due diligence to be conducted and where no business relationship or single transaction should be conducted)

2.16. The following monitoring, mitigating and management controls must apply when

_____

(insert various controls, that apply where a business area is deemed high/medium/low risk, and where a product/service is deemed high/medium/low risk, and on a client level a business relationship is deemed high/medium/low risk. Indicate mitigating and management measures for varying levels of risk)

Customer due diligence controls

3.1. The following individuals are deemed to be prospective clients or clients of the XYZ, _____

(*insert list of scenarios e.g. contracting party in terms of a service agreement or letter of engagement is addressed, natural persons or representatives of legal persons who signs an offer to purchase, both sellers and buyers of an immovable property, individuals that attend legal consultation, the party to whom the invoice is addressed etc*.)

3.2. The following process must be followed to ensure that no anonymous clients, or clients acting under an apparent false or fictitious name may be on-boarded. ____ (*insert process e.g. check whether CDD is completed, where CDD is not required this would only apply for once-off transactions less than R5 000*. *Check that required information is obtained and recorded*).

3.3. When dealing with a client who is conducting a single transaction for an amount less than R5 000 the following information must be obtained and recorded at a minimum: including _____ (*insert information required) (refer to Guidance Note 7*).

3.4. XYZ establishes business relationships or conducts single transactions with the following types of clients_____ (*list different client types e.g. South African natural person, non-resident foreign national natural person, foreign national residing temporarily in South Africa, public and private companies, national government departments, partnerships, trusts etc.*).

3.5. XYZ will not perform a business relationship, or enter into a single transaction with the following types of persons _____

(*list different client types, or specify that there are no such exclusions)*

3.6. When establishing a business relationship, the following information must be obtained: _____ (*list information e.g. nature of business relationship, intended purposes of the business relationship and the source of funds for which the prospective client expects to use in concluding transactions).*

3.7. Simplified due diligence (SDD) may be conducted for all **low-risk** single transactions or business relationships.

3.7.1. When conducting a business relationship *(insert list of SDD information and documents/electronic records)* must be obtained from the client.

3.7.2. When conducting a single transaction *(insert list of SDD information and documents/electronic records)* must be obtained from the client.

3.8. Standard customer due diligence may be conducted for all **medium-risk** single transactions or business relationships.

3.8.1. When conducting a business relationship (*insert list of standard CDD information and documents/electronic records*) must be obtained from the client.

3.8.2. When conducting a single transaction (*insert list of standard CDD information and documents/electronic records*) must be obtained from the client.

3.9. Enhanced due diligence (EDD) must be conducted for all **high-risk** single transactions or business relationships.

3.9.1. When conducting a business relationship (*insert list of EDD information and documents/electronic records*) must be obtained from the client.

3.9.2. When conducting a single transaction (*insert list of EDD information and documents/electronic records*) must be obtained from the client.

3.10. The following table sets out information and documents or electronic records that must be obtained from the client, based upon whether it is a business relationship or single transaction, the risk rating, level of CDD to be conducted and type of client (*insert table for example)*:

ML/TF/PF risk rating	**e.g. indicate client type**	
Low risk – SDD	List information required	List documents/electronic records required
Medium risk – Standard CDD	List information required	List documents/electronic records required
High risk – EDD	List information required	List documents/electronic records required

3.11. The following processes must be followed when conducting CDD on the different types of potential clients, existing clients, persons acting on behalf of the client and beneficial owners _____ (*insert relevant processes e.g. at the on-boarding XYZ employee must request all relevant information and supporting documents/electronic records from the person, review the information and documents/electronic records, capture on the accountable institution's systems, conduct quality control checks, where required obtain management approval for on-boarding, recommended where high-risk business relationships are established obtain senior management approval etc*.).

3.12. When establishing a business relationship, information on the source of funds, the nature of the client's business, and the intended purposes of the business relationship must be obtained in the following manner: _____ (*insert process e.g. application form must request the information*). This information is required regardless of the risk rating. This information must be used by XYZ to determine whether future transactions that will be performed during the business relationship are consistent with the institution's knowledge of the client.

3.13. When establishing a business relationship or conducting a single transaction for clients that are legal persons, trusts and/or partnerships additional due diligence (ADD) must be conducted. Additional due diligence includes establishing the nature of the client's business, establishing the ownership and control structure and identifying the beneficial owner of the client. The additional due diligence process for:

3.13.1. Legal persons include_____ (*state all steps, including name and number of legal person and identifying and verifying the beneficial owner/s) (refer to the process of elimination in FIC Guidance Note 7).*

3.13.2. Trusts include _____ (*state all steps, including name and number of legal person and establishing the identity of the trustees, founder, beneficiaries, determining the Master's Office, and obtaining the trust number)*

3.13.3. Partnerships include _____ (*state all steps, including obtaining name and number of partnership and establishing the identity of each partner*).

3.14. Ongoing due diligence is conducted in respect of business relationships at the following intervals _____ (*insert intervals e.g. annually for high-risk client, every two years for medium risk client and every three years on low-risk clients etc.*). The intervals at which ODD is conducted is dependent on the risk profile of the client.

3.15. In addition, ODD must be conducted when the following scenarios occur _____

(*insert scenarios e.g. during account monitoring a change in client transaction pattern was detected, the accountable institution filed numerous section 29 reports in relation to the client etc.).*

3.16. As part of ODD, the accountable institution must request the following information and documentation/electronic records from the client _____ (*insert all information and documentation*, *this may be the exact same as referred to in paragraph 3.10 above).*

3.17. The following process must be followed when conducting ODD _____ (*insert the process e.g. XYZ staff request latest information and document via e-mail and a courier is sent to collect the required information and documentation etc.)*

3.18. (*This is a recommendation and not mandatory*) Approval must be sought from the _____ senior management before establishing high-risk business relationships in the following manner _____ (*insert the process e.g. e-mail all information and documents to senior manager, who then must either approve/decline. Proof of decision to be maintained on client file*).

3.19. (*This is a recommendation and not mandatory*) The source of wealth information _____ (*insert list of different types of sources of wealth*) must be obtained from a client where it is determined the business relationship is high-risk from an ML/TF/PF perspective.

3.20. XYZ must terminate a business relationship and must not conduct a single transaction where it is unable to conduct CDD, EDD, ADD or ODD. XYZ must consider filing a section 29 report. This must be noted through _____ (*insert applicable process e.g. reporting of non-compliance with all supporting material to be sent to the compliance officer within 2 days)*

3.20.1. The process to terminate a business relationship is as follows _____ (*insert process e.g. escalation of information to senior management, letter sent to client informing client the business relationship will be terminated if the client does not provide document etc.*). The reason for terminating a business relationship must be recorded.

3.21. Where there are doubts regarding the veracity of previously obtained information, the process of CDD, EDD, ADD and ODD where relevant must be repeated. Where something suspicion or unusual becomes apparent while conducting CDD EDD, ADD and ODD, the employee must file a report to the compliance officer.

3.22. Where the XYZ is unable to conduct CDD, it will not establish a business relationship with and or conduct a single transaction for a client. The following process will be followed in these instances _____ (*insert investigation process, termination process*).

Prominent influential persons

(This part applies to business relationships)

4.1. The process of determining whether a person is a DPIP, FPPO, immediate family member or known close associate will be done in the following manner _____ (*insert manner e.g. declaration sought, manually search for information online or automated where the client details is captured in a system of the relevant FPPO and DPIP source lists*).

4.2. Upon establishing a business relationship the following client information ___ (*insert client information e.g. client name, surname, beneficial owner name, person acting on behalf of client's name etc*.) must be scrutinised against the following FPPO and domestic prominent influential persons (DPIP) source lists _____ (*insert source lists relied upon*) in order to determine whether the individual is either a DPIP, FPPO, immediate family member or known close associate.

4.3. The client information must be scrutinised against the FPPO and DPIP source lists at client on-boarding and thereafter at intervals. These intervals are _____ (*insert interval, daily, monthly, every six months etc.*) (*The interval must be proportionate to the ML/TF risk.)*

4.4. Alternatively, XYZ must obtain a declaration from the client indicating whether the client, person acting on behalf of the client or beneficial owner, is a DPIP, FPPO, immediate family member or known close associate. XYZ must record this information on the client file (*e.g. the application form should list the various types*

of DPIPs and FPPOs and require the client to declare their position. Where the client does hold a position of either a DPIP, FPPO, immediate family member or known close associate then senior management approval must be obtained for on boarding etc.)

4.5. XYZ must take reasonable measures to obtain the source of wealth information of an FPPO, high-risk DPIP, their immediate family member or known close associate in the following manner _____ (*insert the reasonable measures e.g. request information through the application form, and request verification documents for the information provided etc*.)

4.6. XYZ must conduct enhanced ongoing monitoring of the business relationship with the FPPO, high-risk DPIP, their immediate family member or known close associate in the following manner _____ (*insert manner e.g. conduct client reviews of account activity on a quarterly basis or at the end of every month etc*.)

4.7. Senior management approval must be obtained before establishing a business relationship with an FPPO, high-risk DPIP, immediate family member or known close associate in the following manner _____ (*set out the process e.g. escalation of all CDD, section 21F, 21G and 21H of the FIC Act information via e-mail to senior management with request to approve/decline the establishment of the business relationship, recording of the e-mail response from the senior management etc*.)

Targeted financial sanctions aimed at terrorist financing

5.1. The following client information _____ (*insert client information, including client name, surname, identity number, registration number, beneficial owner name, person acting on behalf of client name, payment information etc*.) must be scrutinised (screened) against the UN 1267 sanctions list (as published on the UNSC website) in order to identify sanctioned persons (refer to public compliance communication 44).

5.2. The scrutinising will be done in the following manner _____ (*insert method e.g. either using an automated screening system or manually capturing client information in the search tools of the UN 1267 sanctions list*).

5.3. The client information must be scrutinised against the TFS lists and the UN 1267 sanctions list before conducting a single transaction or entering a business relationship, and thereafter at intervals as and when lists are updated or according to the accountable institution's risk-based approach. Intervals include _____ (*insert interval e.g. daily, monthly, every six months etc.)*. The interval must be proportionate to the ML/TF/PF risk.

5.4. The client information must also be scrutinised where updates are made to the TFS lists and UN 1267 sanctions list.

5.5. Where a possible match is found, the client information must be further analysed and compared to determine whether there is a true match (i.e. client is a sanctioned persons) or a false positive (i.e. client has the same name as a sanctioned person but is not the same person). The process for analysing and comparing is_____ (*insert process e.g. XYZ employee will compare the client information against all the sanctioned persons information and determine whether it matches. Where required XYZ will conduct further searches via search engines to source information to determine whether there is a match or not etc.)*

5.6. In an instance where it is a false positive, the reason therefore must be documented, and the on-boarding may continue. This finding, and all information regarding the investigation and decision made that this is a false positive must be kept in the following manner: _____ (*insert process e.g. all material to be saved on the client file and signed off by compliance officer)*

5.7. In an instance where a true positive is found, the reason therefore must be documented and XYZ may not establish a business relationship or conduct a single once-off transaction. This finding, and all information regarding the investigation and decision made that this is a positive match must be kept in the following manner: _____ (*insert process e.g. all material to be saved on the client file and signed off by compliance officer)*

5.8. XYZ must record evidence that client information has been scrutinised against both lists in the following manner _____

(*insert manner e.g. after screening a client's name against the TFS search tool on the Centre's website, the employee will take a screen shot of the results and save the same on the client file etc*.)

Targeted financial sanctions aimed at proliferation financing

6.1. The following client information _____ (*insert client information, including client name, surname, identity number, registration number, beneficial owner name, person acting on behalf of client name, payment information etc*.) must be scrutinised (screened) against the UN 1267 sanctions list (as published on the UNSC website) **and** the targeted financial sanctions lists (TFS list as published on the Centre's website) in order to identify sanctioned persons (refer to public compliance communication 44). XYZ must screen against both lists, as the lists are different.

6.2. The scrutinising will be done in the following manner _____ (*insert method e.g. either using an automated screening system or manually capturing client information in the search tools of the TFS list and UN 1267 sanctions list*).

6.3. The client information must be scrutinised against the TFS lists and the UN 1267 sanctions list before conducting a single transaction or entering a business relationship, and thereafter at intervals as and when lists are updated or according to the accountable institution's risk-based approach. Intervals include _____ (*insert interval e.g. daily, monthly, every six months etc.)*. The interval must be proportionate to the ML/TF/PF risk.

6.4. The client information must also be scrutinised where updates are made to the TFS lists and UN 1267 sanctions list.

6.5. Where a possible match is found, the client information must be further analysed and compared to determine whether there is a true match (i.e. client is a sanctioned person) or a false positive (i.e. client has the same name as a sanctioned person but is not the same person). The process for analysing and comparing is _____ (*insert process e.g. XYZ employee will compare the client information against all the sanctioned persons information and determine whether it matches. Where*

required XYZ will conduct further searches via search engines to source information to determine whether there is a match or not etc.)

6.6. In an instance where it is a false positive, the reason therefore must be documented, and the on-boarding may continue. This finding, and all information regarding the investigation and decision made that this is a false positive must be kept in the following manner: _____ (*insert process e.g. all material to be saved on the client file and signed off by compliance officer)*

6.7. In an instance where a true positive is found, the reason therefore must be documented and XYZ may not establish a business relationship or conduct a single once-off transaction. This finding, and all information regarding the investigation and decision made that this is a positive match must be kept in the following manner: _____ (*insert process e.g. all material to be saved on the client file and signed off by compliance officer)*

6.8. XYZ must record evidence that client information has been scrutinised against both lists in the following manner _____ (*insert manner e.g. after screening a client's name against the TFS search tool on the Centre's website, the employee will take a screen shot of the results and save the same on the client file etc*.)

Account monitoring

7.1. All clients and prospective clients must be profiled according to the following factors _____ (*insert factors according to client type e.g. client income, sector, occupation, products, types, payment methods including cash and EFTs, transaction history where applicable etc.).* Client profiling is required to determine/analyse whether future transactions are consistent with XYZs knowledge of a client. Client profiling aids in the identification of potentially suspicious and unusual transactions or activity.

7.2. XYZ will monitor all account activity and transactions for all business relationships in the following manner _____

(*either manually by reviewing statements daily/as and when transactions occur or automatically through an automated transaction monitoring system*) to identify possible reportable transactions (refer to Directive 5 and PCC 45).

Reporting

8.1. The following process must be followed to identify reportable transactions _____ (*insert process e.g. check statement every day to determine, whether cash transactions above the threshold have been paid or received and whether any suspicious and unusual transactions have taken place etc*.)

8.2. Where reportable transactions are identified, the following process must be applied _____ (*insert process e.g. communicate all the relevant information immediately to the compliance officer and money laundering reporting officers in the prescribed manner, who will then analyse and determine whether it is reportable. State the end-to-end internal process to analyse and report transactions to the Centre, in terms of sections 28, section 28A, and section 29*) (The process must adhere to the reporting periods, refer to Guidance Notes 5B, 4B and 6A).

8.3. Reports made in terms of the FIC Act are confidential.

8.4. The following client and transaction profile scenarios are examples of potential suspicious and unusual transactions in terms of section 29 of the FIC Act_____ (*list all potential red-flag examples e.g. payment of large purchase price in cash, numerous round cash deposits which do not match the client's stated source of income, numerous large electronic transfers made by a third party which does not match the clients stated source of income*). Where these scenarios occur XYZ must conduct further analyses in order to determine whether the transactions/activity is suspicious or unusual or other reportable transactions/activity.

8.5. A terrorist property report in terms of section 28A, must be filed where the accountable institution is in possession or control of property of:

8.5.1. Any entity which has committed or attempted to commit an offence as defined in POCDATARA Act

8.5.2. A specific entity identified in a UN 1267 sanctions list

8.5.3. A person or entity identified in a TFS list as published on the Centre's website

8.6. XYZ will examine complex and unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose, in the following manner _____ (*insert manner e.g. review applications, statements, credit reports, annual financial statements etc.*) by the following persons _____ (*e.g. the compliance officer)* at which interval _____ (e.g. *before concluding a transaction as and when the transaction occurs)* in order to identify as possible reportable transactions.

8.7. XYZ must keep written findings of decisions taken on whether to report or not to report.

8.8. Section 27 requests for information in terms of the FIC Act, will be handled as follows _____ (*insert process, section 42A compliance officer should check the goAML inbox on a daily basis and respond to requests for information on time.*)

8.9. Section 32 requests for additional information in terms of the FIC Act, will be handled as follows _____ (*insert process e.g. section 42A compliance officer should check the goAML inbox on a daily basis and respond to requests for information on time.*) In all instance the CO must be made aware of section 32 requests for additional information immediately upon receipt thereof.

8.10. Section 34 requests for intervention in terms of the FIC Act, will be handled as follows _____ (*insert process e.g. section 42A compliance officer should check the goAML inbox on a daily basis and where a section 34 written directive is received, the CO must ensure all impacted transactions are identified and frozen for the period as stated in the direction.*)

8.11. All reporting information is confidential, XYZ must under no circumstances disclose the contents of a report or the fact that a report has been considered or filed to any other persons. Disclosure of this information is regarded as tipping off, which is an offence.

Record-keeping

9.1. All client information records and transaction records will be stored _____ (*state manner of storage e.g. in a strong room, which is subject to access controls*) at _____ (*insert storage address*) in the following format _____ (*state format e.g. hard copy or electronic copy*) for a minimum period of five years calculated from the date on which the transaction is concluded, or date of termination of a single transaction or a business relationship, or date of report being filed.

9.2. (*Recommendation*) The institution will maintain a register of all reports made to the Centre which will include the date on which the report was made, the person making the report and sufficient information and details regarding the transaction.

9.3. All reports issued on goAML must be downloaded in _____ (*insert for example 1 day*) of submitting the report and kept on record.

9.4. XYZ stores the following records with a third party off-site. The third party's information is as follows _____ (*insert third party's full information, as required in regulation 20 of the Money Laundering and Terrorist Financing Control regulations*) Note, the accountable institution must advise the Centre in writing on a formal letterhead the information as per regulation 20.

Registration

10. XYZ must be registered with the Centre and details must be kept up to date.

10.1. Registration of the following persons must be maintained at all times _____ (*insert names/positions e.g. compliance officer and MLRO if so required)*

10.2. When any information changes, either regarding XYZ's details or any persons holding position of compliance officer or MLRO, this must be updated with the Centre within five business days.

ends

Annexure C: List of indicators that may be used to assess the ML/TF/PF risk

Extract from Guidance Note 7 – paragraph 37

Indicators relating to products and services

- To what extent does the product provide anonymity to the client?
- Does the product enable third parties who are not known to the institution to make use of it?
- Does the product allow for third-party payments?
- Is another accountable institution involved in the use of the product?
- Can the product be funded with cash, or must it be funded only by way of a transfer to or from another financial institution?
- How easily and quickly can funds be converted to cash?
- Does the product facilitate the cross-border transfer of funds?
- Is the offering of the product subject to regulatory approval and/or reporting?
- What does the product enablement process entail and to what extent does it include additional checks such as credit approvals, disclosure of information, legal agreements, licencing, regulatory approvals, registration, involvement of legal professionals, etc?
- To what extent is the usage of the product subject to parameters set by the institution e.g. value limits, duration limits, transaction limits, etc. or to what extent is the usage of the product subject to penalties when certain conditions are not adhered to?
- Is the usage of the product subject to reporting to regulators and/or to “the market”?
- Does historic transaction monitoring information indicate a lower or higher prevalence of abuse of the product for money laundering or terrorist financing purposes?
- What is the intended target market segment for the product e.g.:
    - Entry-level, retail or high-net-worth individuals
    - Larger corporates, SMEs, SOCs, etc.
    - Specific industries, sectors or professions
    - Salaried vs self-employed individuals
    - Minors?

- Is the usage of the product subject to additional scrutiny from a market abuse or a consumer protection perspective?
- What is the time frame for the conversion of funds, property etc. through the usage of the product?
- Is the product an industry-regulated product?
- Does the product allow for the flow of physical cash?
- Are there specific conditions that must be met or events that must take place for clients to have access to funds, property etc.?
- Does the usage of the product entail structured transactions such as periodic payments at fixed intervals or does it facilitate an unstructured flow of funds?
- What is the transaction volume facilitated by the product?
- Does the product have a "cooling off" period which allows for a contract to be cancelled without much formality and a refund of moneys paid?
- Are the products offered over short- or longer-term contractual relationships?
- Do products require a payment from a same-name account or facility to facilitate the opening of a product?

Indicators relating to delivery channels

- Is the product offered to prospective clients directly or through intermediaries?
- Are prospective clients on boarded through direct interaction or through intermediaries?
- Do clients transact by engaging with the institution directly or through intermediaries?
- Where clients interact through intermediaries, are the intermediaries subject to licencing and/or other regulatory requirements?
- Are products and services acquired or transactions performed via an exchange?
- Are products and services traded in secondary markets?
- To what extent does the usage of the product require the participation of the institution or the application of the institution’s systems and transaction platforms?
- What are the payment systems or other technological platforms that support the functioning of the product?
- Are prospective clients on-boarded through non-face-to-face processes and/or do they use the institution’s products and services through non-face-to-face transactions?

Indicators relating to geographic locations

- Is the client domiciled in South Africa or in another country or does the client operate in another country?
- Do clients who are domiciled or operate outside South Africa engage with the institution in South Africa or through branches, subsidiaries or intermediaries outside South Africa?
- Have credible sources identified geographic locations from where clients engage with an institution as high-risk jurisdictions?
- Are the geographic locations from where clients engage with an institution subject to sanctions regimes?
- If the client is a corporate vehicle, has it been incorporated in a country which has been identified by credible sources as a high-risk jurisdiction or in a country which is the subject of a sanctions regime, or does it operate in such a country?
- Has an international body, a domestic regulator, supervisory body or other credible source expressed concern about weak regulatory measures against money laundering and terrorist financing, weak transparency requirements for beneficial ownership of corporate structures or weak institutional frameworks such as supervisory, law enforcement and prosecuting agencies in relation to a geographic location from where clients engage with an institution?
- Are the geographic locations from where clients engage with an institution known to applying excessive client confidentiality?

Indicators relating to clients

- Is the client a natural person or corporate vehicle?
- If the client is a corporate vehicle, is it part of a complex or multi-layered structure of ownership or control?
- What information does the client provide concerning their source(s) of income?
- What is the nature of the client's business activity e.g. does the activity involve transacting in large amounts of cash, cross-border movements of funds, trading in sensitive, controlled or sanctioned commodities, etc?
- What is the nature of the type of the products and services offered by the client?

- Does the client operate solely within the country, or do they have cross-border operations?
- Is the client's product selection rational with a view to support their business or personal needs?
- Does the client occupy a prominent public position or perform a public function at a senior level, or does it have such individuals within its ownership and control structure?
- Is there adverse information about the client available from public or commercial sources?
- Is the client known to be subject to financial sanctions?
- Does the client operate in a sector or industry that is subject to specific standards, market entry or market conduct requirements, other regulatory requirements (especially AML/CFT measures)?
- Is the client supervised for compliance with AML/CFT measures?
- Has the client been penalised or subjected to adverse findings relating to failures to implement AML/CFT measures?
- Has the client been in a business relationship with the institution for a period of time?
- What has been the patterns of transaction behaviour (e.g. speed, frequency, size, volume, etc.) of a client who has a history of a business relationship with an institution?
- Has the institution previously observed suspicious or unusual activities or transactions on the part of the client?

Other factors

- The demographics of a society, its social and economic circumstances, trade dependencies, GDP.
- Financial inclusion objectives and how particular products and services contribute to this.
- The impact of the institution's business strategy on its ML/TF risk profile.
- The ML/TF impact on the institution as a result of having operations in particular jurisdictions (i.e. jurisdictional risk associated with the accountable institution itself, and not its clients).

- The communication of risk factors by authorities based on their understanding of ML/TF risks at a national or sectoral level.
- Trends and typologies identified by the FATF and other international bodies which indicate jurisdictions, structures, products and services, etc. favoured by money launderers and terrorist financiers.
- Anti-fraud measures that may be in place in an accountable institution.
- Consideration of previous regulatory fines.
- Frequency of internal audit findings and the outcomes thereof