Financial
Intelligence Centre

DRAFT GUIDANCE NOTE 7B

ON THE IMPLEMENTATION
OF VARIOUS ASPECTS OF THE
FINANCIAL INTELLIGENCE CENTRE ACT,
2001 (ACT 38 OF 2001)

In collaboration with
the National Treasury,
South African Reserve Bank and
Financial Sector Conduct Authority

12 June 2026

PREFACE

i) The Financial Intelligence Centre (Centre) in collaboration with the National Treasury, South African Reserve Bank and the Financial Sector Conduct Authority (formerly known as Financial Services Board) has published guidance that will be required to support the implementation of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act).

ii) The FIC Act established the Centre which is the national point for the gathering, analysis and dissemination of financial intelligence. The Centre was established to identify proceeds of crime and assist in combating money laundering, the financing of terrorism and proliferation financing and in so doing has a primary role to protect the integrity of South Africa's financial system. The Centre develops and provides financial intelligence to a range of agencies supporting the investigation and prosecution of criminal activity by helping to identify the proceeds of crime, combat money laundering and the financing of terrorism. The FIC Act is a key component of the regulatory architecture that protects the integrity of the South African financial system and (together with legislation such as the Prevention of Organised Crime Act, 1998 (Act 121 of 1998) and the Prevention of Constitutional Democracy against Terrorism and Related Activities Act, 2004 (Act 32 of 2004) of the legal framework that supports the administration of the criminal justice system.

iii) This guidance is issued in terms of section 4(c) of the FIC Act read with regulation 28 of the Money Laundering and Terrorist Financing Control (MLTFC) Regulations which empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations of the Act. Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the MLTFC Regulations issued under the FIC Act. Guidance issued by the Centre is authoritative in nature which means that accountable institutions must take the guidance issued by the Centre into account in respect of their compliance

with the relevant provisions of the FIC Act and the MLTFC Regulations. If an accountable institution does not follow the guidance issued by the Centre, it should be able to demonstrate that it nonetheless achieves an equivalent level of compliance with the relevant provisions of the FIC Act and the MLTFC Regulations. It is important to note that enforcement action may emanate as a result of non-compliance with the FIC Act and the MLTFC Regulations where it is found that an accountable institution has not followed the guidance issued by the Centre.

iv) The guidance provided by the Centre will be updated and revised from time to time. The Centre therefore advises accountable institutions to regularly monitor communications from the Centre so as to stay abreast of the current guidance on a given issue.

Disclaimer

v) 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. This guidance does not provide legal advice and is not intended to replace the FIC Act or the MLTFC Regulations issued under the FIC Act. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

Copyright notice

vi) This guidance is copyright. The material in guidance may be used and reproduced in an unaltered form only for non-commercial use. Apart from any use permitted under the Copyright Act, 1978 (Act 98 of 1978), all other rights are reserved.

Version

vi) Guidance Note 7A was issued on 13 February 2025. This Revised Guidance Note 7A dated 1 September 2025 replaces both Guidance Note 7A and Guidance Note 7 from the date of its publication.

DRAFT GUIDANCE NOTE 7B ON THE IMPLEMENTATION OF VARIOUS ASPECTS OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT 38 OF 2001)

Contents

PREFACE 2

INTRODUCTION 6

CHAPTER 1 ADOPTION OF A RISK-BASED APPROACH 7

I GENERAL PRINCIPLES 7

What is money laundering? 7

What is financing of terrorism? 7

What is proliferation financing?

What is risk? 8

What are inherent and residual risks? 9

Requirement of a risk-based approach in the FIC Act 9

What are money laundering, terrorist financing and proliferation financing risks (ML/TF/PF) risks? 9

What is ML, TF and PF risk management? 10

The effect of a risk-based approach 13

RBA for different industries and sectors 14

II RISK ASSESSMENT and UNDERSTANDING OF RISK 15

ML, TF and PF risk indicators 16

Indicators relating to products and services 17

Indicators relating to delivery channels 19

Indicators relating to geographic locations 19

Indicators relating to clients 20

Other factors 22

Risk-rating 23

The role of a risk matrix 24

III RISK MITIGATION 25

Implementation of systems and controls for management of ML, TF and PF risk 26

Where does customer due diligence fit into risk mitigation? 28

Risk-mitigation measures 28

De-risking and avoiding risk 29
CHAPTER 2 CUSTOMER DUE DILIGENCE MEASURES 31
Introduction 31
Business relationship 32
Single transaction threshold: anonymous clients and clients acting under a false or fictitious names 33
Establishing and verifying clients' identities 34
Establishing and verifying the identities of natural persons 35
Establishing the identity of legal persons, trusts and partnerships 38
Legal persons 38
Partnerships 41
Trusts 42
Impact of the Protection of Personal Information Act, 2013 on the identification and verification requirements of the FIC Act 45
Timing of verification 46
Understanding and obtaining information on the business relationship 47
Ongoing due diligence 48
Doubts about veracity of previously obtained information 49
Inability to conduct due diligence 49
Foreign prominent public officials and domestic prominent influential persons 50
CHAPTER 3 RECORD KEEPING 57
General 57
Obligation to keep customer due diligence records 58
Obligation to keep transaction records 58
Manner in which records must be kept 58
Period for which records must be kept 60
CHAPTER 4 RISK MANAGEMENT and COMPLIANCE PROGRAMME 62
CHAPTER 5 IMPLEMENTATION OF THE UNITED NATIONS SECURITY COUNCIL RESOLUTIONS RELATING TO THE FREEZING OF ASSETS 73
Mechanisms for implementation 73
Screening 74
Accessibility of sanctions list 75
Basic living expenses 75
GLOSSARY 77

DRAFT

INTRODUCTION

1. A country's measures to combat money laundering, terrorist financing and proliferation financing work effectively if the financial system in that country is transparent (based on robust customer due diligence measures) to ensure that adequate information is captured in the records of financial and other institutions and to make the sharing of information that may support further investigation of money laundering, terrorist financing and proliferation financing possible. The purpose of the FIC Act, among others, is to introduce this transparency in the South African financial system.

2. By promoting these focus areas, accountable institutions' compliance with the regulatory requirements of the FIC Act contributes to making it more difficult for criminals to hide their illicit proceeds in the formal financial sector and thereby profiting from their criminal activities and cutting off the resources available to terrorists.

3. The FIC Act incorporates a risk-based approach to compliance elements such as customer due diligence (CDD) into the regulatory framework. A risk-based approach requires accountable institutions to understand their exposure to money laundering, terrorist financing risks and proliferation financing. By understanding and managing their money laundering, terrorist financing risks and proliferation financing risks, accountable institutions not only protect and maintain the integrity of their businesses but also contribute to the integrity of the South African financial system.

DRAFT

CHAPTER 1 ADOPTION OF A RISK-BASED APPROACH

I GENERAL PRINCIPLES

What is money laundering?

5. Money laundering is the manipulation of money or property in order to disguise its true source. Criminal activities, such as drug trafficking, human trafficking, racketeering and corruption generate large amounts of profits for individuals or groups carrying out these activities. When criminals are successful in generating returns from these criminal activities, they obtain illegal earnings that cannot be explained. Therefore, by using funds generated from criminal activities criminals risk drawing the attention of the authorities to the underlying criminal activity thereby exposing themselves to prosecution and forfeiture of the illicit proceeds.

6. In order to benefit from the proceeds of unlawful activity, criminals must conceal the origins of these funds. This is the process of money laundering. The result of a successful money laundering scheme is that proceeds from an underlying unlawful activity are no longer associated with the activity. Unlawfully acquired proceeds therefore appear to be legitimate income.

What is financing of terrorism?

7. The financing of terrorism involves the solicitation, collection and the providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations or individual terrorists. The funds and assets may stem from both legal and illicit sources. The primary goal of persons involved in the financing of terrorism is not to conceal the sources of the funds and assets, as with money laundering, but to conceal both the financing and the nature of the activity being financed.

DRAFT

What is proliferation financing?

7A. Proliferation financing includes any activity which has or is likely to have the effect of providing property, a financial or other service or economic support to a non-state actor, that may be used to finance the manufacture, acquisition, possession, development, transport, transfer or use of nuclear, chemical or biological weapons and their means of delivery. Also, this may include any activity which constitutes an offence in terms of section 49A of the FIC Act.

What is risk?

8. According to international best practice risk rating methodology, risk refers to the likelihood and impact of uncertain events on set objectives. The impact can be either a positive or negative deviation from what is expected. This uncertainty is a function of three factors: Threat, vulnerability and consequence.

9. The context of the above is important. For example, “threat" or “consequence” to whom or what. On the other hand, vulnerability could arise from external and internal factors and may be either controllable or uncontrollable.

10. A threat is a person or group of people, o bject or activity with the potential to cause harm. In the context of money laundering, terrorist financing and proliferation financing this includes criminals, terrorist groups and their facilitators, their funds, as well as the past, present and future money laundering, terrorist financing or proliferation financing activities.

11. The concept of vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. Identifying vulnerabilities, as distinct from threats, means focusing on, for example, the factors that represent weaknesses or features that may be exploited in a given system, institution, product, service etc. The areas in which these vulnerabilities may arise are discussed in more detail later in this guidance.

12. Consequences refer to the impact of a threat or the exploitation of a vulnerability if this impact is to materialise.

13. Risk in the context of money laundering, terrorist financing or proliferation financing can therefore be thought of as the likelihood and impact of money laundering, terrorist financing or proliferation financing activities that could materialise as a result of a combination of threats and vulnerabilities manifesting in an accountable institution.

What are inherent and residual risks?

14. Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied by the accountable institution.

15. Residual risk is the level of risk that remains after controls and mitigation measures were implemented by the accountable institution.

Requirement of a risk-based approach in the FIC Act

16. The FIC Act requires accountable institutions to apply a risk-based approach when carrying out customer due diligence measures.

What are money laundering, terrorist financing and proliferation financing (ML, TF and PF) risks?

17. The concept of ML, TF and PF risks, as the term implies, relate to threats and vulnerabilities that may promote the laundering of proceeds of unlawful activities or the financing of terrorism, on the one hand, or may jeopardise the detection, investigation or prosecution of these activities or the possibility of the forfeiture of proceeds of unlawful activities, on the other.

18. On a national level these are threats and vulnerabilities which put at risk the integrity of South Africa's financial system and negatively impacts the

administration of criminal justice which affects the safety and security of South Africans as well as that of people outside of South Africa.

19. In relation to accountable institutions, ML, TF and PF risks are threats and vulnerabilities which put the accountable institution at risk of being abused in order to facilitate ML, TF and PF activities. These relate to the potential that clients, by using the accountable institution's products and services, can exploit the accountable institution to promote money laundering, terrorist financing or proliferation financing activities. The nature of these risks relate to a number of aspects, including the features of the intended target market of clients who are likely to use an accountable institution's range of products and services, the geographic locations of an accountable institution's operations and of its clients, the delivery channels through which persons become clients of an accountable institution or through which clients access its products and services, the features of a particular product or service, etc. These aspects are discussed in more detail in section II below.

20. In order to have a robust ML, TF and PF risk management system accountable institutions must be able to demonstrate how they contextualise the concepts of "ML and TF risk" within their particular businesses as having an impact on their operational, line management and strategic objectives.

21. Controls should be purposefully built and/or adapted to address ML, TF and PF risks. Accountable institutions may make use of the controls which are already in place.

What is ML, TF and PF risk management?

22. ML and TF risk management is a process that includes the identification of ML, TF and PF risks, the assessment of these risks, and the development of methods to manage and mitigate the risks that have been identified.

23. According to ISO 31000: 2009 (International Organization for Standardization), risk may be managed or dealt with, as follows:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Accepting or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision.

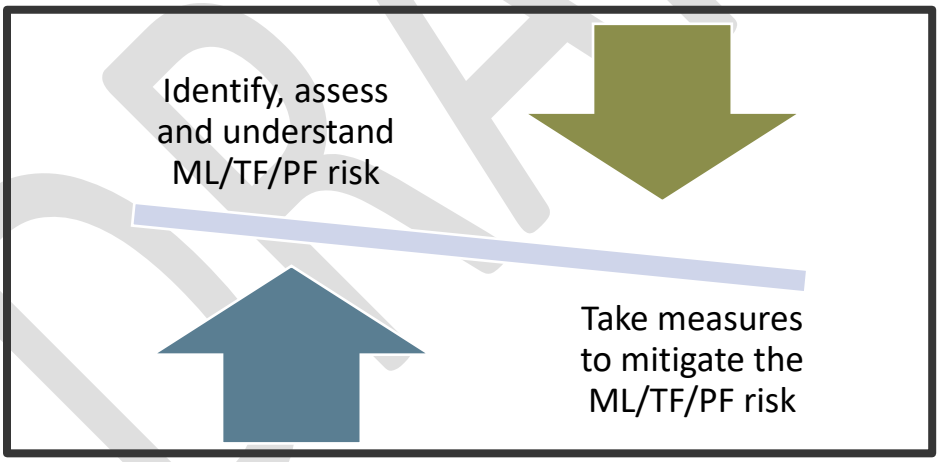
24. These actions apply to ML, TF and PF risk, as with other risks. An accountable institution's risk appetite is a key determining factor in relation to its risk management decisions, in particular the extent to which it will apply resources to treat (mitigate) risks, the extent to which it may tolerate certain risks and the instances when it will avoid or terminate risks. An accountable institution's risk appetite can also differ in relation to different types of risk (e.g. money laundering risk as opposed to terrorist financing risk) or risks arising in different contexts.

25. Management and mitigation of ML, TF and PF risks most probably will entail the treatment of identified risks within an accountable institution. Treating ML, TF and PF risk entails that the accountable institution develops systems and controls to manage the risks identified. These systems and controls should comprise of all the relevant risk mitigation measures at the accountable institution's disposal. The mechanisms which an accountable institution may include in its risk management systems and controls should relate to the nature of particular risks. These mechanisms include the application of customer due diligence measures, the monitoring of business relationships with clients, managing delivery channels for

particular products and services, structuring the features of particular products and services, etc. The potential risk management mechanisms are discussed in more detail later in this guidance.

26. The concepts of "ML, TF and PF risk" and "ML, TF and PF risk management" must always be contextualised within the particular business of an accountable institution, and as having an impact on the operational, line management and strategic objectives of that accountable institution.

27. The application of risk management systems and controls must be commensurate with the extent of assessed risks. This means that the extent to which particular risk management mechanisms are applied in individual cases must bear relevance to consequences of ML, TF and PF risk in particular scenarios in relation to the likelihood and impact of the risk.



28. The process to manage ML, TF and PF risk is a continuous cycle. Accountable institutions should satisfy themselves that their ML, TF and PF risk management systems and controls remain adequate in view of changing circumstances relating to emerging threats and vulnerabilities, product innovations, new target markets, changes in circumstances of individual clients or classes of clients, etc.

Accountable institutions should also ensure that their ML, TF and PF risk management systems and controls are adhered to within that institution.

29. This means that accountable institutions should reassess ML/TF risks, in particular residual risks after the application of ML, TF and PF risk management systems and controls, at regular intervals. The institutions should then review the continued adequacy of its ML, TF and PF risk management systems and controls on the basis of these regular assessments.

The effect of a risk-based approach

30. By applying a risk-based approach accountable institutions are able to ensure that measures to prevent or mitigate money laundering, terrorist financing and proliferation financing are commensurate with the risks identified. This will ensure that resources are directed in accordance with priorities, so that the greatest risks receive the highest attention. The risk-based approach also affords accountable institutions the flexibility to use a range of mechanisms to establish and verify the identities of their clients, creating opportunities for accountable institutions to explore more innovative ways of offering financial services to a broader range of clients and bringing previously excluded sectors of society into the formal economy. If applied correctly, it will improve the efficacy of measures to combat money laundering, terrorist financing and proliferation financing while promoting financial inclusion without undermining AML, CFT and CPF objectives. Accountable institutions should also ensure alignment between Treating Customer Fairly principles and its application of guidance on ML, TF and PF risk issues.

31. The risk-based approach further allows accountable institutions to simplify the due diligence measures applied where they assess ML, TF and PF risks to be lower. Instead of relying on rigid requirements in regulations and exemptions granted at the executive level, accountable institutions will have greater discretion to determine the appropriate compliance steps to be taken in given instances, in

accordance with their internal AML, CFT and CPF compliance and risk management programmes.

Risk-based approach for different industries and sectors

32. Different industries or sectors have different exposures to ML, TF and PF risk. The Centre will, in the future and as the need arises, consider specific guidance to address industry or sector specific challenges when implementing the risk-based approach.

DRAFT

II RISK ASSESSMENT AND UNDERSTANDING OF RISK

33. Assessing ML, TF and PF risk requires accountable institutions to identify the ML, TF and PF risks they may face in the context of their businesses and to analyse these with a view to understand how the identified ML, TF and PF risks affects them. The likelihood of a risk transpiring as well as the impact of such a risk should also be considered by the accountable institution. This implies that accountable institutions must have adequate processes, proportionate to their size and complexity, to identify and assess ML, TF and PF risks.

34. The mechanisms used in a particular accountable institution to assess ML, TF and PF risk must be proportionate to the size and complexity of the institution. The risk assessment process therefore might be quite simple or very sophisticated depending on the size and structure of the accountable institution and the nature and range of products and services it offers.

35. The processes within accountable institutions to identify and assess ML, TF and PF risks must take account of a range of factors which may be indicative of greater or lesser threats and vulnerabilities to money laundering, terrorist financing and proliferation financing in a given scenario. Factors that are indicative of increased threats or vulnerabilities have been shown, based on previous experience, to lend themselves more readily to abuse by criminals.

36. Accountable institutions may have access to and may use various databases to assess the ML, TF and PF risks relating to their clients. The context within which accountable institutions assess ML, TF and PF risks is also influenced by ML, TF and PF risks that are identified at a national level in all the jurisdictions where they operate. Accountable institutions should therefore determine in their risk assessment processes what weight they give to risks identified at national level in the relevant jurisdictions where they operate. The sources of information on risk

indicators and the processes for their consideration should be described in an accountable institution's risk management and compliance programme (RMCP).

ML, TF and PF risk indicators

37. Factors that may be indicative of ML, TF and PF risks relate to several aspects such as product or service features, delivery channels, geographic areas etc. Each of these may interact differently with the characteristics of different types of clients. The examples of factors that may be indicative of ML, TF and PF risk provided here are not an exhaustive or prescriptive list and institutions must also consider other factors that may be relevant to their own organisations or sectors. Furthermore, the examples provided here are phrased in neutral terms, a factor may be indicative of either higher or lower ML, TF and PF risk depending on the context within which it is considered. It is therefore important that accountable institutions can demonstrate how they bring different indicators to bear on a given scenario to reach an appropriate risk classification.

37A. Accountable institutions should identify and assess the ML, TF and PF risks that the development of new products, new business practices, new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products pose. This assessment should be reflected in the institution's risk assessment processes and RMCP.

DRAFT

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 usage 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 processes entail and to what extent does it include additional checks such as credit approvals, disclosure of information, legal agreements, licensing, regulatory approvals, registration, involvement of legal professionals, etc?
- To what extent is the usage of the product subject to parameters set by the institution that e.g. value limits, duration limits, transaction limits, etc. or to what

DRAFT

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, terrorist financing or proliferation financing purposes?
- What is the intended target market segment for the product for example.
    - "Entry-level", "retail" or "high net worth individuals"
    - Larger corporates, SME's, SOC's, 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 consumer protection perspective?
- What is the time duration 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 happen 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 short term or longer-term contractual relationships?
- Do products require a payment from a same name account or facility to facilitate the opening of a product

DRAFT

Indicators relating to delivery channels

38. The delivery channel refers to the means by which institutions and clients interact with each other in the offering of products and services, onboarding of clients and the usage of products and services.

- 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 institutions 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 outside of South Africa or operate outside South Africa engage with the institution in South Africa or through branches, subsidiaries or intermediaries outside South Africa?

DRAFT

- 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 jurisdictions 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 or supervisory body or other credible source expressed concern with weak regulatory measures against money laundering, terrorist financing and proliferation 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

39. It is trite that not all clients of an accountable institution pose the same ML, TF and PF risk. For an accountable institution to accurately identify all the factors that may be relevant to a particular client and to include all those factors in an assessment of ML, TF and PF risks, it is necessary that the institution has a holistic view of the information gathered about the client across all the points of engagement between the institution and the client. This implies that an accountable institution which offers a range of products and services should consider the different engagements with a particular client in relation to different products and services as component parts of one relationship with that client and assess the ML, TF and PF risks relating to that relationship in a holistic manner.

40. An assessment of ML, TF and PF risks relating to clients could entail an assessment for each individual client or for groups of clients fitting the same profile. Where an accountable institution evaluates the characteristics of a group of clients as part of a risk assessment, the institution should ensure that any individual client to whom the characteristics of the group are ascribed, actually meets the profile of that group.

40A. For example, under-served or low income persons should not as a whole be deemed to automatically pose a lower risk of ML, TF and PF, a comprehensive risk assessment must be conducted before it is concluded that certain business relationships or single transactions with clients or category of clients present a low risk.

- 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 and CPF measures)?
- Is the client supervised for compliance with AML, CFT and CPF measures?
- Has the client been penalised or subjected to adverse findings relating to failures to implement AML, CFT and CPF 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

41. In addition to the characteristics of products and services, delivery channels, geographic locations and clients mentioned above there are also other factors which institutions should take into account when assessing ML, TF and PF risks. These are contextual factors which, on the one hand, may contribute to a more accurate assessment of ML, TF and PF risks in relation to particular business relationships or categories of relationships, or assist in determining an institution's risk appetite in relation to particular business relationships or categories of relationships, on the other.

- 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 and PF risk profile.

- The ML, TF and PF 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 and PF 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, terrorist financiers or proliferation 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.

42. The Minister of Finance has issued a number of exemptions from compliance with a range of requirements under the FIC Act which applied to accountable institutions before the amendments to the FIC Act took effect. The changes brought about by these amendments necessitated the withdrawal of many exemptions in addition to substantial amendments to the MLTFC Regulations, made under the FIC Act. Despite the withdrawal of these exemptions, accountable institutions may be guided by their content as additional factors that may indicate lower ML and TF risks in a given scenario.

Risk-rating

43. Risk-rating implies assigning different categories to different levels of risk according to a risk scale and classifying the ML and TF risks pertaining to different relationships or client engagements in terms of the assigned categories. As no two accountable institutions are the same, the level of risk and therefore the risk ratings attributed to particular business relationships or other engagements with clients may vary between accountable institutions.

44. A risk scale should be tailored according to the size of the accountable institution and consideration may be given to criteria set out in international best practice. The complexity of the risk scale should reflect the size and complexity of the accountable institution and the nature and the range of products and services it offers to its clients.

45. Accountable institutions offering a relatively homogenous range of products and services, using a limited range of delivery channels, operating in one or a few geographic location(s) or engaging with a homogenous range of clients require relatively simplistic risk scales distinguishing only between two or three risk categories. However, accountable institutions offering a more diverse range of products and services, using a wider range of delivery channels, operating in a larger number of geographic locations or engaging with a more diverse range of clients require more finely calibrated risk scales distinguishing between a larger number of risk categories.

46. The ML and TF risk associated with a particular client engagement is not static. The factors underlying any given risk-rating will inevitably change over time. It is therefore essential that accountable institutions re-evaluate the relevance of particular risk factors and the appropriateness of previous risk-ratings from time to time and determine the intervals at which this will be done.

47. Accountable institutions must document their risk-rating methodology and procedures which they apply as well as the conclusions reached through the processes in the accountable institution's RMCP. This includes the criteria and the intervals for the re-evaluation of risk-ratings.

The role of a risk matrix

48. The assessment of ML and TF risk should ultimately draw together all the factors that are relevant to an engagement with a client. A risk matrix could serve as a tool to provide an objective basis to the assessment of several risk indicators. A risk

matrix may be made up of different components in order to evaluate a particular client, transaction, product or service in its entirety.

49. Extensive guidance on risk matrices has been developed internationally which may assist accountable institutions when developing a risk management framework. Examples of these include:

- Matrix of events, products and services, clients, etc. that lead to inherent ML and TF risks.
- Matrix of internal control activities applied by the accountable institution in mitigating ML and TF risks. This may be used to help guide the selection of appropriate control actions in relation to the risk.
- Matrix of residual risks which will indicate levels of comfort as to whether or not the accountable institution has done enough to manage the probability, likelihood and impact of such a risk occurring.

III RISK MITIGATION

50. Risk mitigation in the context of ML, TF and PF refers to the activities and methods used by an accountable institution to control and minimise the ML, TF and PF risks it has identified. An accountable institution should therefore apply its knowledge and understanding of its ML, TF and PF risks in the development of control measures to mitigate the risks identified.

51. The risk assessment process will therefore assist accountable institutions in determining the nature and extent of resources necessary to mitigate identified risks.

52. Whether a particular risk is adequately addressed will be determined by whether the level of residual risk is acceptable and within the risk appetite of the accountable institution.

53. It is important to note that the risk-based approach does not exempt an accountable institution from applying effective AML, CFT and CPF controls. It is the responsibility of accountable institutions to effectively manage all ML, TF and PF risks.

54. Accountable institutions must establish and implement systems and controls in response to the assessed risks. These controls must be designed to detect money laundering, terrorist financing and proliferation financing and respond appropriately when risks materialise.

55. Where there are higher ML, TF and PF risks, enhanced measures must be taken to mitigate those risks. This means that the range, degree, frequency or intensity of preventive measures and controls conducted will be stronger in higher risk scenarios.

56. Where the ML, TF and PF risks are assessed as lower, simplified measures may be applied. This means that controls must include certain CDD measures, but that the degree, frequency and/or the intensity of the controls conducted will be relatively lighter.

Implementation of systems and controls for management of ML, TF and PF risk

57. An accountable institution's systems and controls should provide for more information to be obtained about their clients, more secure confirmation of clients' information to be applied and closer scrutiny to be conducted to their clients' transaction activities where they assess the risk of abuse to be higher. This is referred to as enhanced due diligence.

58. By the same token, an accountable institution's systems and controls may allow for less information to be obtained, less secure confirmation of information to be

applied and less frequent scrutiny to be conducted where they assess the risk of abuse to be lower. This is referred to as simplified due diligence.

58A. Simplified due diligence includes a basic level of identification and verification that is applied when a business relationship or single transaction poses a low risk of money laundering, terrorist financing and proliferation financing. Accountable institutions must not apply simplified due diligence where there is a suspicion of ML, TF and PF, as the business relationship or single transaction would automatically pose a high risk in this scenario. Where there is a suspicion of ML, TF and PF the accountable institution must conduct enhanced due diligence and file a report in terms of section 29 of the FIC Act.

59. An accountable institution should always have grounds on which it can base its justification for a decision that the appropriate balance was struck in a given circumstance.

60. The systems and controls by which an institution decides to manage ML, TF and PF risks and the levels of due diligence it chooses to apply in relation to various risk levels must be documented in its RMCP.

61. The risk-based approach is not a "zero failure" approach as there may be instances where an accountable institution has taken all reasonable measures to identify and mitigate ML, TF and PF risks, but is still exploited for money laundering, terrorist financing or proliferation financing. It is important that each institution has adequate detection and reporting measures in place to address ML, TF and PF risks.

62. Mechanisms to manage risk may include but are not limited to:

- Systems, policies and procedures - to be included in the RMCP
- Awareness training of staff
- Reporting channels

- Client analytics
- Process to exit from high-risk relationships
- Approval procedures for higher risk transactions and relationships
- Adequate supervision for higher risk activities and
- Screening tools.

How does customer due diligence fit into risk mitigation?

63. Institutions should use the customer due diligence process as one of the measures to mitigate the ML, TF and PF risk associated with a proposed business relationship or single transaction. The customer due diligence process provides an accountable institution with the information required to know who they are doing business with, to know who benefits from the business it does with its clients, to understand the nature of the business it does with its clients and to determine when the business with clients should be considered suspicious or unusual. This is one of the mechanisms at accountable institutions' disposal to mitigate the risk of exploitation for money laundering, terrorist financing or proliferation financing purposes.

64. Customer due diligence measures are discussed in full in Chapter 2.

Risk mitigation measures

Measures that may be applied in cases of higher ML, TF and PF risk
• Increased automated transaction monitoring
• Increased intensity of CDD measures
• Increased review periods of client information
• Utilising more or higher quality sources for the vetting of information (impacts both quality and quantity)
• Senior management involvement in decisions to on-board clients
• Dedicated specialist staff managing enhanced due diligence for specific clients

- Limited reliance on another accountable institution's controls.

De-risking and avoiding risk

65. It should be noted that conducting high-risk activities or having high-risk business relationships is not prohibited anywhere in the FIC Act. Defining clients and products or services as high-risk does not cast a negative light on the accountable institutions nor on the clients and products and services.

66. Risk assessment does not imply that institutions should seek to avoid risk entirely (also referred to as de-risking) through, for example, wholesale termination of client relationships for certain sectors.

67. De-risking poses a threat to financial integrity in general and to the risk-based approach, specifically, as it creates opacity in the affected persons' or entities' financial conduct and it eliminates the possibility to treat ML, TF and PF risks.

68. Wholesale refusal of services or termination of services to a class of clients, for example, termination of correspondent banking relationships with specific categories of financial institutions, may give rise to financial exclusion risk. It may also give rise to reputational risk.

69. The Centre views the wholesale termination or restriction of business relationships to avoid risk, rather than treat the risk, as an example of inadequate risk management. Instead, accountable institutions should take into account the level of ML, TF and PF risk of each client and any applicable risk mitigation measures whether these are implemented by the financial institution or the client. Measures to mitigate risk should be applied accordingly.

70. Avoiding risk by refusing services or terminating or restricting business relationships should be used a measure of last resort where an accountable

institution has reached a conclusion that ML, TF and PF risks relating to specific clients cannot be mitigated adequately or effectively.

DRAFT

CHAPTER 2 CUSTOMER DUE DILIGENCE MEASURES

Introduction

71. Customer due diligence (CDD) refers to the knowledge that an accountable institution has about its client and the institution's understanding of the business that the client is conducting with it.

72. CDD measures, if properly implemented, enables an accountable institution to better manage its relationships with clients and to better identify possible attempts by clients to exploit the institution's products and services for illicit purposes. Requiring accountable institutions to apply CDD is a key component of a framework to combat money laundering, terrorism financing and proliferation financing effectively.

73. Previously accountable institutions were required to establish and verify the identity of a client in accordance with the MLTFC Regulations. The principle of client identification and verification is now expanded significantly with the introduction of the obligation to conduct CDD. As a result, the regulations and exemptions relating to client identification and verification have been amended significantly to align with the amendments to the FIC Act, with most of the regulations having been repealed and exemptions having been withdrawn.

74. This, combined with the obligation to apply a risk-based approach (as discussed in Chapter 1 above), gives accountable institutions greater discretion to determine the appropriate compliance steps to be taken in given instances. This means that accountable institutions now have the flexibility to choose the type of information by means of which it will establish clients' identities and also the means of verification of clients' identities, instead of following the rigid steps provided for in the MLTFC Regulations.

DRAFT

75. Accountable institutions should use the findings from their risk assessment to decide on the appropriate level and type of CDD that they will apply to a client (or business relationship and single transactions). Accountable institutions should also determine when they consider persons to be prospective clients to whom their CDD measures apply. An accountable institution's RMCP must describe the CDD measures which the institution applies and how these measures are attenuated or intensified on the basis of ML, TF and PF risks.

Business relationship

76. A business relationship is defined in the FIC Act as an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis. A business relationship therefore entails an element of a time duration to the engagement with the client.

77. Accountable institutions need to determine what constitutes a business relationship as well as a transaction in the context of their particular business for purposes of complying with the obligations of the FIC Act in as far as it applies to a business relationship.

78. The manner and the point in time at which an accountable institution determines that a person is a prospective client or a client for the purposes of determining when the obligations of the FIC Act commence should be spelled out in an accountable institution's RMCP, both in respect of a business relationship and a single transaction. The accountable institution should therefore determine, taking into account its particular business, who is to be regarded as a prospective client and client in order to apply the CDD and other requirements in terms of the FIC Act.

Single transaction threshold: Anonymous clients and clients acting under a false or fictitious names

79. The FIC Act defines a single transaction as a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5 000 (the amount is determined by the Minister of Finance in the Regulations). This can be described as occasional or once-off business where there is no expectation on the part of the accountable institution or the client that the engagements would recur over a period of time.

80. Institutions need to determine what constitutes a single transaction in the context of their particular business for purposes of complying with the obligations of the FIC Act in as far as it applies to single transactions.

81. Accountable institutions are not required to carry out the full scope of CDD measures in respect of clients conducting single transactions below the value to be set by the Minister of Finance in the MLTFC Regulations. However, the threshold for single transactions does not apply to the obligations set out in section 20A of the FIC Act. This means that, in spite of a single transaction being below the threshold, the accountable institution is still prohibited from dealing with an anonymous client or a client with an apparent false or fictitious name. As a result, in such cases, the accountable institution should obtain and record at least some information describing the identity of the client even if that information does not have to be verified. Examples of information to be obtained could include the full name and identity number of the client and other information such as a contact number. An added step of requesting to view an identification document of the client is advisable. The manner in which the accountable institutions comply with section 20A of the FIC Act in respect of business relationships and single transactions, both below and above the threshold, must be recorded in the institution's RMCP.

DRAFT

Establishing and verifying clients' identities

82. CDD starts with an accountable institution knowing the identity of its client. In terms of section 21 of the FIC Act an accountable institution must, in the course of establishing a business relationship or entering into a single transaction, establish and verify the identity of the client and, if applicable, the person representing the client as well as any other person on whose behalf the client is acting. The objective of this provision is that an accountable institution, after applying its processes to establish and verify a client's identity, should have confidence that it knows who the client is with sufficient certainty given the accountable institution's risk assessment pertaining to that client engagement.

83. Establishing a client's identity entails that an accountable institution obtains a range of information about the client. In most cases this information is provided by the client in response to questions being asked by the accountable institution as part of its on-boarding process (in the case of a business relationship) or its client engagement process (in the case of a single transaction). Verification of the client's identity entails that the accountable institution corroborates the person's identity information by comparing this information with information contained in documents or electronic data issued or created by reliable and independent third-party sources.

84. As indicated in Chapter 1 above, large parts of the MLTFC Regulations, (in particular Chapter 1 of the Regulations which described the methods which accountable institutions had to use to establish and verify their clients' identities) have been repealed. Accountable institutions must now choose the type of information by means of which they will establish clients' identities and also the means of verification of clients' identities. The nature and extent of verification of clients' identities must be determined taking the assessed ML, TF and PF risks associated with the relevant business relationship or single transaction into account. These decisions as to how the accountable institution goes about the identification and verification of its clients, as well as how these measures are

attenuated or intensified based on ML, TF and PF risk, must be described in the accountable institution's RMCP.

Establishing and verifying the identities of natural persons

85. A natural person's identity can be determined by reference to a number of attributes. At the very basic level these attributes are the person's full names, date of birth and, in most cases, a unique identifying number issued by a government source (e.g. in the case of a South African citizen or resident, his/her identity number or, in the case of other natural persons, a passport number or numbers contained in asylum seeker or refugee permits, work permits, visitors' visas etc.). It is expected that these basic attributes will always be used in accountable institutions' processes to establish a natural person's identity.

86. Information about a natural person's identity may be supplemented by applying other attributes of a natural person including his/her physical appearance or other biometric information, place of birth, family circumstances, place of employment or business, residential address, contact particulars (e.g. telephone numbers, e-mail addresses, social media), contacts with the authorities (e.g. tax numbers) or with other accountable institutions. This list of examples is not exhaustive and there may be other attributes of particular persons or categories of persons which accountable institutions may include in their identification processes. The nature and amount of other attributes which an accountable institution applies in a given case is dependent on the extent to which the institution relies on the verification of the client's identity as a means to mitigate ML, TF and PF risk in that case (see the discussion on risk mitigation in Chapter 1 above).

87. Verification methods vary and are mostly dictated by the type of information used to establish a person's identity in a given scenario. Regardless of the method applied, it is important that verification be done using information obtained from a reliable and independent third-party source and, as far as possible, the original source of the information. Accountable institutions should evaluate the adequacy

of corroboration of a person's identity attributes. This implies that institutions must determine the level of confidence they have that any particular method of corroboration provides certainty as to the relevant identity attributes. A factor that accountable institutions should bear in mind in this context, is the controls which are applied to ensure that information reflected in a particular source is accurate. Information sources created or generated by the client him/herself are not considered to be reliable and independent third-party sources.

88. Government issued or controlled sources of information such as various forms of identity documents (e.g. South African identity documents including smart card identity documents, driver's licenses, foreign identity documents, passports, asylum seeker or refugee permits, work permits, visitors' visas) and the underlying electronic databases where information evidenced in identity documents are kept, are most often the original sources of information concerning the relevant attributes and therefore provide a high level of confidence as a means to corroborate a natural person's basic identity attributes. Hence, accountable institutions should, as far as practicable, use government issued or controlled sources as the means of verification when verifying basic identity attributes. Accountable institutions should only in exceptional cases use information obtained from sources other than the original source of the information (e.g. where the original source is not available) and this should only be done in cases where accountable institutions are confident that they can adequately manage ML, TF and PF risks.

89. Corroboration of a person's identity in relation to both basic and other identity attributes can be in documentary or electronic form. Moreover, many of a person's identity attributes accumulate over time and can be found in the person's so-called "electronic footprint". With this in mind the Centre encourages accountable institutions to make use of information in electronic form to corroborate a prospective client's information against multiple third-party data sources.

90. Accountable institutions making use of electronic data sources to verify a prospective client's identity remain responsible and accountable in their own capacity for compliance with the requirements of the FIC Act. The use of electronic data sources in the verification process does not provide automatic indemnity from regulatory action relating to the institution's compliance with these requirements. It is important therefore that accountable institutions apply due diligence in choosing electronic solutions as a means to enable verification of a prospective client's identity.

91. If accountable institutions make use of electronic data sources they should apply the same test in principle as in the case of documentary sources, i.e. that the sources should be reliable and independent third-party sources and as, far as possible, the original source of the relevant information. Accountable institutions should likewise determine the level of confidence they place in particular electronic sources of corroboratory information. Solutions which allow prospective clients to manipulate source information in any manner should not be considered credible information sources to enable verification of clients particulars.

92. A factor that may contribute to an accountable institution's confidence in corroboration based on electronic sources is the size of a person's "electronic footprint" in relation to the depth, breadth and quality of electronic information. This implies that accountable institutions would have a greater level of confidence in corroboration from electronic sources if they use information from multiple sources, and across time.

93. The means of verification and the sources of corroboration an accountable institution uses in a given case are dependent on the extent to which the institution relies on the verification of the client's identity as a means to mitigate ML, TF and PF risk in that particular case (see the discussion on risk mitigation in Chapter 1 above).

94. Examples of sources of information that may corroborate a person's identity attributes include records of the Department of Home Affairs, records of the Companies and Intellectual Property Commission, records of the South African Revenue Service, eNaTIS records and records of the Master of the High Court.

Establishing the identity of legal persons, trusts and partnerships

95. Section 21 of the FIC Act (the requirement to establish and verify a client's identity) also applies to clients who are not natural persons acting in their personal capacity. Clients of this nature are referred to as corporate vehicles and include legal persons, trusts and partnerships. In addition to the obligation to establish and verify the identities of corporate vehicles, section 21B of the FIC Act also require accountable institutions to apply additional due diligence measures namely to establish:

- the nature of the client's business
- the ownership and control structure of the client and
- the beneficial ownership of clients, and

to take reasonable steps to verify the identity of the beneficial owners. The requirements to establish and verify the identities of corporate vehicles and to apply the additional due diligence measures are discussed separately in respect of legal persons, partnerships and trusts or similar arrangements in the sections that follow.

96. The requirements set out in sections 21 and 21B of the FIC Act apply whether the legal person, partnership or trust or similar arrangement between natural persons is incorporated or originated in South Africa or elsewhere.

Legal persons

For additional guidance please refer to public compliance communication 59.

97. A legal person is defined in the FIC Act as any person, other than a natural person, that establishes a business relationship or enters into a single transaction with an

accountable institution and includes a person incorporated as a company, close corporation, foreign company or any other form of corporate arrangement or association but excludes a trust, partnership or sole proprietor.

98. Examples of attributes which describe a legal person's identity include:

- The name under which the legal person has been incorporated;
- Its form, e.g. whether it is a company or a close corporation;
- The registration number under which it is incorporated, if applicable;
- The address of its registered office;
- The powers that regulate and bind the legal person;
- Its directors or members, as may be applicable;
- Its senior management e.g. its chief executive officer;
- Its trading name if it is different from the name under which it has been incorporated;
- Its business address if it is different from the address of its registered office; and
- Its income tax or value added tax numbers.

99. The attributes used to establish a legal person's identity must be sufficient to prove the existence of the legal person and describe the legal person's identity. The nature and amount of the attributes which an accountable institution applies in a given case are dependent on the extent to which the institution relies on the verification of the client's identity as a means to mitigate ML, TF and PF risk in that particular case (see the discussion on risk mitigation in Chapter 1 above). This must be described in the institution's RMCP.

100. As in the case of natural persons, it is important that verification be done using information obtained from a reliable and independent third-party source and, as far as possible, the original source of the information be used to corroborate a legal person's identity attributes. The remarks made in paragraphs 88 to 94 above

concerning the verification of identity also apply with regard to legal persons. Accountable institutions should therefore give preference to using sources of information that are created or controlled by public sector institutions, such as the information held by the Companies and Intellectual Property Commission be used to corroborate attributes associated with the incorporation of companies.

101. In addition to establishing and verifying a legal person's identity an accountable institution also must establish the nature of the legal person's business and its ownership and control structure. Furthermore, an accountable institution must also establish who the beneficial owner of the legal person is and take reasonable steps to verify the beneficial owner's identity.

102. (Refer to public compliance communication 59)

103. (Refer to public compliance communication 59)

104. Once the accountable institution has determined who the beneficial owner of a legal person is, the institution must take reasonable steps to verify that person's identity. The remarks made above about the verification of a natural person's identity also apply in this instance. The reference to "reasonable steps" confirm that accountable institutions must apply measures that are commensurate with the assessed ML, TF and PF risk in a given case to the verification of the beneficial owner's identity. This includes making use of information obtained by reasonably practical means while striking a balance between the accuracy of the verification required, on the one hand, and the level of effort invested in the means to obtain such verification on the other. The different measures which an accountable institution uses to verify the identities of beneficial owners of legal persons must be described in the institution's RMCP. The underlying element of this requirement is that the accountable institution must be satisfied that it knows who the beneficial owner is.

105. (Refer to public compliance communication 59)

Partnerships

106. Refer to public compliance communication 59 for guidance on beneficial owners of partnerships. Partnerships are not incorporated entities and do not have legal personality. However, accountable institutions must establish the identities of partnerships who are their clients nonetheless. This means that the starting point to the identification of a partnership is to determine how the partnership is generally known. Accountable institutions must therefore establish whether a partnership is identified by a unique name or description. In addition to establishing this information, accountable institutions must take reasonable steps to verify it. This means that accountable institutions must apply measures that are commensurate with the assessed ML, TF and PF risk relating to a partnership in a given case. Examples of information that can be used for this purpose include the partnership agreement which establishes the partnership and governs its membership and functioning, business correspondence of the partnership and promotional material advertising the partnership's business. The measures which an accountable institution uses to verify the identities of partnerships must be described in the institution's RMCP.

107. The concept of a beneficial owner in the context of a partnership encompasses all the partners in the partnership. Hence, section 21B(3) of the FIC Act requires accountable institutions, over and above the requirements of sections 21 and 21A of the FIC Act, to establish the identity of every partner in a partnership. This includes every member of a partnership en commandite (a partnership where the liability of certain partners who contribute a fixed amount and who remain undisclosed as partners, is limited according to the partnership agreement establishing and governing the partnership), an anonymous partnership (a partnership where the partners' names are not disclosed to persons who are not partners in the partnership) or any similar partnership.

108. The express references to partnerships en commandite and anonymous partnerships indicates clearly the intention that accountable institutions must establish the identity of every person who contributes to a partnership or may benefit from a partnership when they do business with a partnership. The most reliable source document indicating who the members of the partnership are, is the partnership agreement which establishes the partnership and governs its membership and functioning.

109. Section 21B(3) of the FIC Act also requires accountable institutions to establish the identity of the person who exercises executive control over the partnership, if there is such a person, indicating that accountable institutions should determine the notion of control over (in addition to benefit from) a partnership. Moreover, the provision requires accountable institutions to establish the identity of each natural person who is authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of a partnership.

110. Accountable institutions are required to take reasonable steps to verify the names of the natural persons covered by section 21B(3) FIC Act. The remarks made above about the verification of a natural person's identity also apply in this instance. Again here the reference to "reasonable steps" confirm that accountable institutions must apply measures to verify the relevant persons' identities that are commensurate with the assessed ML, TF and PF risk in a given case. The different measures which an accountable institution uses to verify the identities of the relevant natural persons must be described in the institution's RMCP. The underlying element of this requirement is that the accountable institution must be satisfied that it knows the identities of the relevant natural persons.

Trusts

111. Refer to public compliance communication 59 for guidance on beneficial owners of trusts. As in the case of partnerships, trusts are not incorporated entities and do

not have legal personality. All trusts in South Africa are "express trusts" – either trusts *inter vivos* (trusts created during the lifetime of a person) or *mortis causa* trusts (trusts created in terms of the will of a person and comes into effect after their death). The administration of trusts in South Africa is regulated by the Trust Property Control Act, 1988.

112. The FIC Act defines a 'trust' as any trust as contemplated in the Trust Property Control Act, 1988 but excludes trusts established-

- by virtue of a testamentary disposition;
- by virtue of a court order;
- in respect of persons under curatorship; or
- by the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund.

113. However, it is important to note that the definition of trusts includes a similar arrangement established outside the Republic.

114. The identification and verification requirements set out in section 21B(4) of the FIC Act apply in respect of a trust which is *inter vivos.* The existence of a trust must be registered at an office of the Master of the High Court before legal effect can be given to the trust and the trustee(s) can obtain authority from the Master of the High Court to perform their functions. Therefore, accountable institutions must establish the unique reference number identifying the trust in the Master's Office and the address of the Master of the High Court where the trust is registered as part of the elements describing the identity of the trust.

115. In respect of foreign trusts, accountable institutions should obtain a letter of authority or other official document from a competent trust registering authority in a foreign jurisdiction.

116. In addition to establishing this information, accountable institutions must take reasonable steps to verify it. This means that accountable institutions must apply measures that are commensurate with the assessed ML, TF and PF risk relating to a trust in a given case. The most reliable source of confirmation for this information is the trust deed (the agreement which establishes the trust and governs its functioning) and the information controlled (and documentation issued) by the relevant offices of the Masters of the High Court. The measures which an accountable institution uses to verify the identities of trusts must be described in the institution's RMCP.

117. The concept of a beneficial owner in the context of a trust encompasses all the natural persons who may benefit from a trust arrangement or may control decisions in relation to the management of trust property or are otherwise associated with the trust. Hence, section 21B(4) of the FIC Act requires accountable institutions, over and above the requirements of sections 21 and 21A of the FIC Act, to establish:

- The identity of each founder;
- If a founder of the trust is a legal person or a person acting on behalf of a partnership or in pursuance of the provisions of a trust agreement, the beneficial owner of that legal person, partnership or trust
- The identities of each trustee and each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the trust, and
- If a trustee is a legal person or a person acting on behalf of a partnership, the beneficial owner of the legal person or partnership
- Each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the accountable institution on behalf of the trust, whether such a person is appointed as a trustee for the trust or not

DRAFT

- The identities of each beneficiary referred to by name in the trust deed or other founding instrument in terms of which the trust is created; or
- If a beneficiary referred to by name in the trust instrument is a legal person or a person acting on behalf of a partnership or in pursuance of the provision of a trust agreement, the beneficial owner of the legal person, partnership or trust
- If beneficiaries are not referred to by name in the trust deed or other founding instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined.

118. Accountable institutions are required to take reasonable steps to verify the names of the natural persons covered by section 21B(4) of the FIC Act. The remarks made above about the verification of a natural person's identity also apply in this instance. Again here the reference to "reasonable steps" confirm that accountable institutions must apply measures to verify the relevant persons' identities that are commensurate with the assessed ML, TF and PF risk in a given case. The different measures which an accountable institution uses to verify the identities of natural persons associated with trusts must be described in the institution's RMCP. The underlying element of this requirement is that the accountable institution must be satisfied that it knows the identities of the relevant natural persons. Paragraphs 82 and 85 should be applied in respect of establishing the identity of a client that is a trust that is excluded from the definition of a trust.

Impact of the Protection of Personal Information Act, 2013 on the identification and verification requirements of the FIC Act

119. The processing of personal information of clients for the purposes of the FIC Act compliance may only be done within the confines of the Protection of Personal Information Act, 2013 (the POPI Act). While the processing and further processing of personal information of a client for purposes of FIC Act requirements is allowed in terms of the (POPI Act), accountable institutions should be cautious of verifying

clients' identities using third party data sources which may have obtained personal information about a client without the client's consent or knowledge.

Timing of verification

120. A client's identity and, where applicable, the identities of beneficial owners and other persons associated with a client, must be verified in the course of conducting a single transaction or entering into a business relationship. This means that an accountable institution may initiate the processes related to the conclusion of a single transaction or entering into a business relationship while it is verifying the relevant persons' identities, but the institution must complete the verification before the institution concludes a transaction in the course of the resultant business relationship or performs any act to give effect to the resultant single transaction.

121. This implies that accountable institutions may, for example, accept a mandate from a prospective client to establish a business relationship or to conclude a single transaction or take any similar preparatory steps with a view of establishing a business relationship or concluding a single transaction before completing verification of the identities of the prospective client and other relevant persons. However, in doing so accountable institutions must take care not to incur unmitigated ML, TF and PF risks by, for example, receiving funds from a client which may have to be returned to the client before completing the verification or making funds available to a client before completing the verification.

122. The manner and processes for the identification of clients and verification of their identities described in an accountable institution's RMCP must also provide for the timing of verification and the mitigation of ML, TF and PF risks where verification is not completed before a single transaction is conducted or a business relationship entered into.

Understanding and obtaining information on the business relationship

123. Section 21A of the FIC Act requires accountable institutions to ascertain from a prospective client what the nature and intended purpose of the business relationship will be, as well as to obtain information on the source of funds that the prospective client expects to use in the course of the business relationship. The purpose of section 21A of the FIC Act is to understand the nature of the client and the envisaged business relationship between the client and the accountable institution. By complying with this provision an accountable institution should be able to form a view of the frequency and the nature of transactions that could be expected to be conducted in the normal course of the ensuing business relationship. This understanding also contributes to the accountable institution's understanding of the ML, TF and PF risk associated with the particular business relationship.

124. In most cases, the purpose and intended nature of the business relationship will be self-evident given the nature of the product or service that the client is requesting.

125. The manner and type of information obtained in terms of section 21A of the FIC Act must be recorded in the accountable institution's RMCP. Information that may be relevant include-

- The nature and details of the client's business/occupation/employment;
- The expected source and origin of the funds to be used in the business relationship; and
- The anticipated level and nature of the activity that is to be undertaken during the business relationship.

126. The information which an accountable institution obtains from a prospective client should be sufficient for the institution to form the intended understanding of the client and the business relationship. Accountable institutions may form this understanding by accepting the information obtained for this purpose at face value.

Accountable institutions are not required to verify the veracity of the information obtained under section 21A of the FIC Act.

Ongoing due diligence

127. Section 21C of the FIC Act provides for ongoing due diligence measures. These measures follow on from the obligation to understand the purpose and intended nature of a business relationship. They include the scrutiny of transactions undertaken throughout the course of a relationship, to ensure that the transactions being conducted in the course of a business relationship are consistent with an accountable institution's knowledge of the client, and the client's business and risk profile, including, where necessary, the source of funds. It also requires accountable institutions to ensure that the information that an accountable institution has about a client is still accurate and relevant.

128. The objective of the ongoing measures is to identify activities of clients during the course of the business relationship which are not consistent with the accountable institution's knowledge of the client, or the purpose and intended nature of the business relationship, and which need to be assessed for the possibility that the institution may have grounds to report a suspicion of money laundering, terrorist financing or proliferation financing. Accountable institutions should pay particular attention to complex or unusually large transactions and all unusual patterns of transactions which have no apparent business or lawful purpose. If the accountable institution suspects that a transaction or activity is suspicious or unusual and the institution believes that performing the ongoing due diligence requirements will disclose to the client that a report will be made in terms of section 29 of the FIC Act, the accountable institution may discontinue the ongoing due diligence process and consider making a report in terms of section 29 of the FIC Act.

129. The intensity and frequency of ongoing due diligence in respect of a given business relationship must be determined on the basis of the accountable institution's

understanding of ML, TF and PF risks associated with that relationship. An accountable institution must include, in its RMCP, the manner in which and the processes it will have in place to conduct ongoing due diligence and account monitoring of business relationships.

130. Additionally, the institution must include, in its RMCP, the manner in which it will examine complex or unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose as well as how it will keep the written findings of such transactions.

Doubts about veracity of previously obtained information

131. Section 21D FIC Act provides for measures that accountable institutions are required to take if doubts about the veracity or adequacy of previously obtained customer due diligence information arise later on in the relationship, or where a suspicion of money laundering, terrorist financing or proliferation financing is formed at a later stage.

132. An accountable institution is required to repeat the steps set out in sections 21 and 21B of the FIC Act in accordance with its RMCP and to the extent that is necessary to confirm the information that is required to be verified.

133. An accountable institution must provide, in its RMCP, for the manner in which and the processes by which the institution will confirm information relating to a client when it has doubts about the veracity of previously obtained information.

Inability to conduct due diligence

134. Section 21E of the FIC Act prohibits accountable institutions from entering into or maintaining business relationships or concluding single transactions if they cannot perform the required CDD in accordance with the provisions of the Act. This provision must be applied against the background of the remarks made in paragraphs 120 to 121 above on the timing of verification.

135. Accountable institutions should take an objective approach when considering what constitutes an inability to conduct CDD in any particular situation. There may be circumstances where it is reasonable to delay discontinuing a business relationship while the institution facilitates the client's efforts to rectify the failure. The reasonableness of such a delay will vary depending on the circumstances of each case. Where a client refuses to provide requested documentation or information the business relationship should be discontinued once the client has been informed of the potential implications and given time to respond accordingly.

136. Accountable institutions should give special consideration to whether the circumstances that prevent them from conducting CDD are suspicious or unusual as required in section 29 of the FIC Act.

137. The sequence of attempts to obtain the required information or to apply other CDD measures needs to be spelled out in an accountable institution's RMCP. In this context the accountable institution's RMCP must also indicate at what point in the process of entering into a business relationship or concluding a single transaction the verification of a prospective client's identity should be completed and at which point the conclusion will be reached that the institution is not able to conduct appropriate CDD of the required information is not forthcoming. Additionally, an accountable institution's RMCP must provide for the manner in which it will terminate an existing business relationship when it is unable to complete the CDD requirements.

Foreign politically exposed persons, domestic politically exposed persons and prominent influential persons

For additional reference please refer to:
http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

138. Sections 21F, 21G and 21H of the FIC Act deal with politically exposed persons and prominent influential persons. The starting point for the effective implementation of measures relating to persons who are entrusted in prominent public or private sector positions, is for accountable institutions to have effective measures in place to know who their clients are and to understand their clients' business.

139. Business relationships with domestic politically exposed persons or prominent influential persons are not inherently high-risk. Accountable institutions must consider each such relationship on its own merits in order to determine whether there is any reason to conclude that it brings higher risk of abuse for money laundering, terrorist financing and proliferation financing purposes. If so, the accountable institution must apply the same requirements as for foreign politically exposed persons.

140. Business relationships with foreign politically exposed persons must always be considered high-risk. If an accountable institution finds out that it is dealing with a foreign politically exposed persons, senior management approval must be obtained to establish the business relationship. Accountable institutions must also take reasonable measures to establish the source of wealth and source of funds of the client and conduct enhanced ongoing monitoring of the business relationship. Accountable institutions are not required to verify the information about the client's source of wealth and source of funds, but will have to include this information in its client profile which will be used as the basis for enhanced ongoing monitoring. These requirements also apply to immediate family members and known close associates of such politically exposed persons and prominent influential persons.

141. The notion of senior management in an accountable institution is determined by the size, structure, and nature of the institution. The appropriate level of seniority for approval should also be determined by the level of increased risk associated

with the business relationship. The senior manager approving a business relationship with a politically exposed person or prominent influential person should have sufficient seniority and oversight to take informed decisions on issues that directly impact the institution's risk profile.

142. When considering whether to approve a business relationship with a politically exposed person or prominent influential person, senior management should base their decision on the level of ML, TF and PF risk the institution would be exposed to if it entered into that business relationship and how well equipped the institution is to manage that risk effectively.

143. The responsibility regarding final decisions on business relationships with politically exposed persons or prominent influential persons should be clearly described. In all cases, it is best to document the approval or refusal by those involved in writing.

144. When determining the source of wealth, an accountable institution should look at the activities that have generated the total net worth of the client (that is, the activities that produced the client's funds and property).

145. When determining the source of funds, an accountable institution should consider the origin and the means of transfer for funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends).

146. A person is considered to be a domestic politically exposed person if he or she holds, including in an acting position for a period exceeding six months or has held a prominent public function in the Republic of South Africa as listed in Schedule 3A to the FIC Act.

147. The definition of prominent influential person includes an individual who holds or has held at any time in the preceding 12 months a position as listed in Schedule 3C to the FIC Act.

Note: It is envisaged that the Minister of Finance will delay the operational date of Schedule 3C in the legislation, given that information about persons who may fall in this category is not publicly available currently. The National Treasury will explore ways to make such information readily available to enable easier compliance by accountable institutions.

148. The definition of a foreign politically exposed person incudes an individual who holds, or has held in any foreign country a prominent public function as listed in Schedule 3B to the FIC Act.

149. (Removed).

150. The client remains the most valuable source of information in order to determine whether he/she occupies a position of politically exposed person or prominent influential person. Accountable institutions may augment the information obtained from its client by making use of commercially available information sources which specialise in providing information on prominent and politically exposed persons if there is a need to conduct more thorough checks, or if there is a high likelihood of an accountable institution having politically exposed persons or prominent influential persons as clients.

151. Commercial databases are not necessarily comprehensive and have not necessarily been assessed for the quality of the information they provide. The use of commercially available information sources to establish whether a person occupies a politically exposed or prominent influential position therefore does not provide automatic indemnity from regulatory action relating to the institution's compliance with these requirements. It is the responsibility of the accountable

institution to ensure that commercial databases used by the institution to identify persons in politically exposed or prominent influential positions are comprehensive enough to detect such persons.

152. It is recommended as good practice to make use of the internet and other available information sources also to further test the reliability and completeness of client information. This includes reference to media articles and internet search engines.

153. Section 21H of the FIC Act provides that the measures for politically exposed persons and prominent influential persons also apply to their immediate family members and known close associates.

154. Immediate family members of a politically exposed person or prominent influential person include-

- The spouse, civil partner and life partner;
- The previous spouse, civil partner or life partner;
- Children and step children and their spouse, civil partner or life partner;
- Parents; and
- Siblings and step siblings and their spouse, civil partner or life partner.

155. Close associates are individuals who are closely connected to a politically exposed person or prominent influential person, either socially or professionally. The term "close associate" is not intended to capture every person who has been associated with a politically exposed person or prominent influential person. Examples of known close associates extracted from guidance provided by the FATF include the following types of relationships:

- Known sexual partners outside the family unit (e.g. girlfriends, boyfriends, mistresses);
- Prominent members of the same political party, civil organisation, labour or employee union as the politically exposed or prominent person;

- Business partners or associates, especially those that share (beneficial) ownership of corporate vehicles with the politically exposed or prominent person, or who are otherwise connected (e.g., through joint membership of a company board).
- Any individual who has sole beneficial ownership of a corporate vehicle set up for the actual benefit of the politically exposed or prominent person.

156. Accountable institutions are required to determine if they are dealing with a family member or known close associate of a politically exposed person or prominent influential person regardless of whether the politically exposed person or prominent influential person is a client of the accountable institution or not.

157. It is recognised that there is generally less information available to accountable institutions about family members and known close associates of politically exposed persons or prominent influential persons, making the determination as to whether a client (or prospective client) falls in one of these categories more challenging. Accountable institutions should refer to what is known publically about a politically exposed person or prominent influential person's sphere of influence in order to determine if a client is a family member or known close associate of a prominent person in addition to having regard to the information about their clients which is in their possession already. To this end accountable institutions can make use of commercially available sources of information that outlines associations of politically exposed persons or prominent influential persons, monitoring of the media, credible third-party sources of information and information that may be available from other institutions within the same group which are doing business in other countries as well as applying existing processes already in place for purposes such as ongoing monitoring of business relationships.

158. The remarks made in paragraphs 150 and 152 above on the sources of information about politically exposed persons or prominent influential persons also apply in respect of family members and known close associates.

159. Accountable institutions should bear in mind that although a client might not initially (at the commencement of the business relationship) meet the definition of a politically exposed person or prominent influential person (or immediate family member or known close associate), this position might change over time. Likewise an accountable institution may only become aware of the fact that a client is a family member or close associate of a politically exposed person or prominent influential person after he or she has become a client of the accountable institution, e.g. when the accountable institution conducts on-going due diligence of its existing clients. Therefore accountable institutions should, as far as practicable, be alert to public information relating to possible changes in the status of their clients.

160. Accountable institutions must provide, in their RMCPs, how they determine whether a prospective client is a foreign politically exposed person, domestic politically exposed person or prominent influential person (including the sources of information they use) and how they assess and mitigate the money laundering, terrorist financing and proliferation financing risks associated with business relationships with officials and persons. This includes the processes which accountable institutions implement in respect of existing clients where a client's status as a politically exposed person or prominent influential person has changed after the start of the relationship with the client or where accountable institutions were not aware of a client's status as family member or close associate of a politically exposed person or prominent influential person.

CHAPTER 3 RECORDKEEPING

General

161. Recordkeeping is an essential component of a successful system to combat money laundering, terrorist financing and proliferation financing. Often the records of clients' identities and their transaction activities would be the only evidentiary trail to assist law enforcement authorities in the detection, investigation, prosecution and confiscation of criminal funds where illicitly flows of funds are concerned. Recordkeeping is therefore the other side of the coin to CDD measures and together these two elements bring greater transparency to the financial system. It is for this reason that the FIC Act requires accountable institutions to retain records concerning client identification and transaction activity.

162. Meeting the record-keeping requirements will ensure that adequate information is captured in an accountable institution's records to enable the reconstruction of a trail of transactions with a view to assist investigators in determining flows of funds when performing their investigative functions. Against this background it is helpful for accountable institutions to keep their reporting obligations under the FIC Act in mind when determining internal processes and systems for record-keeping so as to ensure that all relevant information is readily available and that reporting under the FIC Act is not unduly delayed or impeded by a lack of available information.

163. The record-keeping requirement is not dependent on risk levels and it is fully applicable to the CDD, transaction and other information collected, whatever the range of this information may be. All the elements of an accountable institution's record management processes which give effect to the requirements of the FIC Act must be referenced in the accountable institution's RMCP.

DRAFT

Obligation to keep customer due diligence records

164. Section 22 of the FIC Act provides for an obligation on accountable institutions to keep customer due diligence records.

165. This means that accountable institutions must keep record of all information pertaining to a client obtained in the course of its processes to comply with sections 21 to 21H of the FIC Act. Such records must include copies of, or references to, information provided to or obtained by the accountable institution to verify the person's identity.

Obligation to keep transaction records

166. Accountable institutions must keep transaction records of single transactions and transactions concluded in the course of the business relationship with the client in terms of section 22A of the FIC Act.

167. This means that the accountable institution must keep records of every transaction which that accountable institution has with a client. Transaction records must be sufficient to enable the transaction to be reconstructed and include the amount, currency, date of transaction, parties to the transaction, the nature of the transaction, pertinent or relevant business correspondence and also the identifying particulars of all accounts and account files related to the transaction if the accountable institution provides account facilities.

Manner in which records must be kept

168. The FIC Act is not prescriptive as to the manner in which records must be kept. This implies that records may be stored in accordance with an accountable institution's standard procedures for the capture of information and the retention of records. Records can therefore be kept by way of storing original documents, photocopies of original documents, scanned versions of original documents or otherwise in computerised or electronic form.

169. There are many examples of mechanisms which may be used for the storage of records which allow accountable institutions to reduce the volume and density of records such as:

- Internal networks
- Physical storage devices e.g. hard drives, CDs, DVDs, memory sticks, etc.
- Cloud storage
- Electronic document repositories
- Fintech capabilities.

170. Regardless of the manner in which records are kept, accountable institutions must ensure that the following principles are met:

- The accountable institution must have free and easy (in other words unencumbered) access to the relevant records;
- The records must be readily available to the Centre and the relevant supervisory body when required;
- The records must be capable of being reproduced in a legible format and
- If the records are stored off-site the Centre and the relevant supervisory body must be provided with the details of the third party storing the records.

171. It is advisable that records include details that will assist in the identification of the records such as:

- Reference numbers on documents or letters;
- Relevant dates, such as issue or expiry;
- Details of the issuer or writer.

172. Accountable institutions must ensure that records are tamper proof and that there are safeguards in place to prevent the unauthorised access to information stored electronically.

DRAFT

173. Accountable institutions which operate in groups of companies may implement group-wide policies on record-keeping which may include centralised storage of records. Accountable institutions should bear in mind that the principles mentioned in paragraph 170 above also apply where record keeping is centralised within a group. This is particularly important if the location of the centralised storage of records is outside of South Africa. No secrecy provisions or data protection legislation should restrict the South African based accountable institution(s)' free and easy access to the relevant records, or result in the records not being readily available to the Centre or relevant South African supervisory bodies or law enforcement authorities. If restrictions exist in another jurisdiction, where records are kept which would impede such access to the records, the relevant records or copies thereof must be kept in South Africa.

174. It is advisable for accountable institutions which make use of commercial third party services, or intra-group centralised data storage to retain their records to conduct regular assessments of its service providers and to test the controls and business processes so as to provide assurance to the relevant supervisory body that the accountable institution can access and retrieve data and/or documents as envisaged under the FIC Act.

Period for which records must be kept

175. Records in relation to establishment of a business relationship referred to in section 22 of the FIC Act must be kept for at least five years from the date on which the business relationship is terminated.

176. Records of all transactions concluded referred to in section 22A must be kept for at least five years from the date on which that transaction is concluded.

177. Records of a transaction or activity which gave rise to a report contemplated in section 29 of the FIC Act must be kept for at least five years from the date on which the report was submitted to the Centre.

178. It is advisable that accountable institutions keep records which to their knowledge relate to ongoing investigations until the relevant law enforcement agency has confirmed that the case has been closed, where possible.

179. Accountable institutions must be mindful of these periods for which records under the FIC Act must be kept if their procedures for the retention of records also provide for the destruction of records.

DRAFT

180. Accountable institutions must develop, document, maintain and implement a risk management and compliance programme (RMCP) for anti-money laundering (AML), counter-terrorist financing (CTF) and counter proliferation financing (CPF). The accountable institution's RMCP documentation must record all the elements of the programme as set out in section 42 of the FIC Act.

181. It is important that accountable institutions acknowledge in their RMCPs that the board of directors (where the accountable institution is a legal person with a board of directors), or the senior management of an accountable institution without a board of directors, is ultimately responsible for ensuring that the accountable institution implements and complies with their RMCPs.

Role of the board of directors, senior management, or the persons with the highest level of authority in the accountable institution

Responsibilities relating to approval and compliance

181A. The accountable institution's board of directors, or senior management, or the person(s) with the highest authority must **approve** the RMCP and **ensure compliance** by the accountable institution and its employees with the provisions of the FIC Act and its RMCP.

181B. An accountable institution that is a legal person must have a compliance function and assign a person with sufficient competence and seniority to assist the board of directors or senior management in complying with the FIC Act and their RMCP. An accountable institution that is not a legal person (except a sole proprietor) must appoint a person with sufficient competence as the compliance officer.

181C. The obligation to approve the RMCP and accountability of the board of directors, senior management, persons or group of persons with the highest authority of an accountable institution that is a legal person, cannot be delegated to other persons, group of persons, employees, committees or structures within the accountable institution. The RMCP must be approved by the board of directors, where there is no board of directors the senior management itself, where there is no senior management the person with the highest level of authority and cannot be delegated to any other persons.

Example 1: Obligation and accountability of the board cannot be delegated
The board of directors of Bank K must approve the RMCP, the board cannot delegate its obligations in terms of the FIC Act. The board may have a committee that provides advice on the suitability of the RMCP, however, the committee cannot take the decision to approve the RMCP. The obligation to approve the RMCP remains with the board.

181D. Where an accountable institution that is a legal person does not have a board of directors, the obligation for approval of the RMCP and accountability of the senior management or person or group of person(s) with the highest authority, cannot be delegated to other persons, employees, committees or structures within the accountable institution.

181E. Where the accountable institution is a sole proprietor, the obligation for approval of the RMCP and accountability of the person(s) with the highest authority cannot be delegated to another person or group of persons.

Adequacy of RMCP approval

181F. The RMCP must adequately address the full scope of section 42 of the FIC Act. The board of directors, senior management or other person(s) with the highest authority should ensure that the RMCP is **adequate, suitable and effective** for the accountable institution.

181G. The RMCP must be described comprehensively in the documentation tabled for approval by the board of directors, senior management or person(s) with the highest authority. The RMCP documentation should not merely reference other documents but must include an adequate and substantial description of the elements of the RMCP.

181H. The accountable institution must be able to demonstrate that there is sufficient information in the RMCP documentation to enable the board, senior management and the person(s) with the highest authority, to apply their minds to determine whether the RMCP is adequate for the accountable institution.

181I. The RMCP documentation must include substantial information that would enable the board, senior management or person(s) with the highest authority, to gain full appreciation for the ML, TF and PF risks the accountable institution faces and the controls that are in place to mitigate and manage the risk, and whether the RMCP enables compliance by the accountable institution with its obligations as set out in the FIC Act.

181J. Where the RMCP documentation does not sufficiently describe the RMCP, it cannot be demonstrated that the board of directors, senior management or person(s) with the highest authority have applied their minds to determine whether the RMCP complies with section 42 of the FIC Act. This may be indicative of non-compliance with section 42(2B) and section 42A of the FIC Act.

181K. A board of directors, senior management or person(s) with the highest authority who demonstrates an underdeveloped understanding of the accountable institution's RMCP will be unable to discharge their obligation in terms of section 42A(1) of the FIC Act.

181L. The RMCP documentation provided to the Centre or supervisory body, on request or during an inspection, must include the approval of the RMCP by the board of directors, senior management or person or group of person(s) with the highest authority.

181M. An inadequate RMCP and RMCP documentation provided to the Centre or supervisory body, may constitute non-compliance with the FIC Act and may lead to administrative sanctions being imposed. The board of directors, senior management or other person or group of person(s) with the highest authority may be sanctioned in terms of section 61 of the FIC Act.

Example 2: Inadequate RMCP

During an inspection, Bank M provides RMCP documentation which does not describe the bank's risk-based approach, neither does it adequately detail the bank's specific inherent and residual ML, TF and PF risks. Bank M thereafter seeks to add further documentation, which did not form part of the documentation that was provided to the board for approval.

In this scenario a supervisory body could conclude that the board of directors did not discharge its responsibility of determining whether the RMCP adequately addresses the ML, TF and PF risk. Further that the board of directors did not ensure compliance with the FIC Act and approve an adequate RMCP.

Culture of compliance

182. The board of directors, senior management or person(s) with the highest authority should ensure that a culture of compliance within the accountable institution is maintained, including ensuring that the accountable institution's policies, procedures and processes are designed to identify, assess, monitor, mitigate and

control risks of ML, TF and PF and are fully consistent with FIC Act obligations and that employees adhere to them.

183. The board of directors, senior management and person(s) with the highest authority is solely responsible for the adequateness of the RMCP and will be held accountable if the RMCP is found to be inadequate.

Example 3: Approval of an RMCP without adequate application of mind

Bank O's AML, CFT and CFP risk committee approved the RMCP documentation, and the board approved the committee's decision without having reviewed and applied their minds to determine whether the RMCP sufficiently and adequately enables compliance with the FIC Act as well as manages and mitigates the ML, TF and PF risk. This constitutes non-compliance by the board of directors, in terms of its obligations with the FIC Act.

Example 4: Inadequate RMCP documentation

During an inspection, financial services provider M (FSP M) provides RMCP documentation that is merely an outline and does not provide a description of the RMCP which has been approved by the board of directors.

This scenario may indicate that FSP M's RMCP has not been approved by the board. This may constitute non-compliance with the board of director's obligations in terms of the FIC Act.

Example 5: Version control

During an inspection, financial services provider Q (FSP Q) provides the approved RMCP to the supervisory body. However, after the approval of the RMCP, FSP Q updated and implemented a revised RMCP that has not been approved by the board of directors. This scenario may constitute non-compliance by the board of directors in terms of its obligations with the FIC Act.

Elements of an effective RMCP and the documentation of an RMCP

183A. Sections 42(1), 42(2) and 42(2A) of the FIC Act indicates what must be included in an accountable institution's RMCP. The Centre recommends that the RMCP documentation includes the following three parts as a minimum:

Part 1 – Identification and assessment of the risk the accountable institution faces of being abused for ML, TF and PF (e.g. the risk-based approach assessment, methodology, framework, entity, product and service offerings, developing technologies, delivery mechanisms, enablement processes, business processes and client risk assessments etc.) as well as an indication of the accountable institution's risk tolerance level or appetite.

Part 2 – Mitigation and management of risks identified through applying appropriate controls, including customer due diligence (CDD), reporting and record keeping, etc.

Part 3 – Monitoring whether the controls implemented are adequate and effective to mitigate and manage the risks as identified and assessed.

Risk identification

183B Accountable institutions must first conduct an entity wide AML/CFT/CFP risk assessment to identify the ML, TF and PF risks the accountable institution faces, before determining the controls required to mitigate the risk, which controls form part of the RMCP. Before the board approves the RMCP, the board must consider whether the RMCP adequately mitigates the ML, TF and PF risk, therefore the board must be satisfied that an entity wide AML/CFT/CFP risk assessment has been conducted, and all the relevant risk factors have been taken into account

183C The accountable institution's entity wide AML/CFT/CFP risk assessment is an important first step in ensuring that an appropriate RMCP can be

developed, as it should be comprehensive enough to enable an accountable institution to clearly identify, assess and appreciate the inherent and residual ML, TF and PF risks and threats it faces. This includes taking into account the nature, size, products, service offerings, industry, client base, geographic location(s), complexity of business, delivery mechanisms, third party service providers and any other relevant factors of the accountable institution.

183D. Where the accountable institution forms part of a group, separate entity risk assessments should be conducted by each accountable institution, which should feed into the group's entity wide AML/CFT/CFP risk assessment. An accountable institution should clearly indicate in the RMCP, whether all accountable institutions that form part of a group structure have been covered when conducting the group entity wide AML/CFT/CFP risk assessment. The entity wide AML/CFT/CFP risk assessment must adequately cover all of the accountable institution's businesses, products, service offerings, technologies, delivery mechanisms, enablement processes, business processes and client base etc.

183E. The risk assessments should also be informed by published national and sector risk assessments that must be reflected in the RMCP as applicable to the business of the accountable institution.

Documentation considerations

183F. The RMCP documentation constitutes the identifiable and readily accessible information that comprehensively records the RMCP. The accountable institution must make the RMCP available to employees and also use it for training. Importantly, it would be the documentation provided to the FIC or other supervisory body, on their request, for examination purposes in terms of section 42(4) of the FIC Act.

DRAFT

183G. RMCP documentation must reference related documentation that constitutes and enables the full implementation of the RMCP. Documentation that is not referenced in the RMCP is not considered to be part of the RMCP.

184. The RMCP documentation should include a description of the board of directors, senior management or person(s) with the highest authority, and a description of the compliance function that assists. The RMCP documentation should also include a description of the seniority and experience of the person who assists in ensuring compliance with the FIC Act.

184A. The accountable institution's RMCP documentation should also cover, among other aspects:

- Appropriate training on ML, TF and PF to ensure that employees are aware of and understand their legal and regulatory responsibilities and their role in handling possible criminal information or property and ML, TF and/or PF risk management.
- Appropriate provision for regular and timely information to the board of directors, senior management or person(s) with the highest authority relevant to the management of the institution's ML, TF and PF risks.
- Appropriate documentation of the institution's risk management policies, risk assessment methodologies and risk profile in relation to ML, TF and PF, including documentation of the institution's application of those policies.
- Appropriate descriptions of decision-making processes regarding different categories of customer due diligence and other risk management measures, including escalation of decision-making to higher levels of seniority in the accountable institution where necessary.
- Appropriate measures to ensure that ML, TF and PF risks are escalated and considered in the day-to-day operation of the institution, including in relation to:

- The development of new products, services, delivery mechanisms, practices and technologies
- Taking on or onboarding of new clients
- Ongoing monitoring of business relationships
- Changes in the institution's entity wide AML/CFT/CFP risk assessment profile.

185. An accountable institution's RMCP must be commensurate with the size, complexity and the nature of the institution's business. This implies that the RMCP for an accountable institution which does not provide a wide range of products and/or services, or which does not deal with a diverse range of clients, could be relatively simple. Complex financial institutions which provide a wide range of products and services or that deal with a diverse range of clients would be expected to have a much more complicated and multi-faceted RMCP.

185A. An accountable institution is required to indicate in the documentation of its RMCP whether any of the elements described in section 42 of the FIC Act do not apply to that particular institution. The institution is also required to indicate in its RMCP why such processes are not applicable to the institution or what alternative control measures have been implemented.

186. The nature and extent of an accountable institution's internal systems and controls which form part of its RMCP depends on a variety of factors, including:

- The nature, scale and complexity of the accountable institution's business
- The diversity of its operations, including geographical locations
- Its client, product or services profile
- Its distribution channels, delivery mechanisms, and use of technology
- The value, volume and size of its transactions
- The degree of risk associated with each area of its operations.

187. Accountable institutions which operate in groups of companies may implement group-wide RMCPs. In doing so, accountable institutions must ensure that the various elements of group-wide RMCPs, including internal processes, systems and controls are appropriate for the different entities or branches within the group and are adequately tailored to specific entities or branches within the group, commensurate with their individual risks, where necessary. The group-wide RMCP should indicate what elements are applicable to different entities and what is not applicable to different entities within the group and why this is so.

188. Accountable institutions situated in South Africa and operating in foreign jurisdictions should also be aware of the local AML, CFT and CFP obligations in all jurisdictions where they operate. This should be reflected in the accountable institution's RMCP document. Procedures should be in place to meet local AML, CFT and CFP obligations in each jurisdiction where an accountable institution operates. If there are variations or conflicts between the South African and the foreign jurisdiction's AML, CFT and CFP compliance requirements, and if the foreign jurisdictions requirements would result in a lower standard than in South Africa, the accountable institution must implement measures which meet the South African requirements. Unless there is a reason that prevents the accountable institution from doing so, then the accountable institution must inform the supervisory bodies, and take into consideration the level of risk in the foreign jurisdiction and apply appropriate additional measures to manage the risk.

189. It is important that the RMCP and the content of an accountable institution's documentation of their RMCP is communicated widely throughout the institution, as may be applicable, and the implementation thereof monitored consistently and audited periodically to increase the effectiveness of its implementation.

190. An accountable institution must review its RMCP at regular intervals to ensure that it remains relevant to the institution's operations and the identified risks. The

review, and any amendments made to the RMCP must be documented and approved as described above.

190A. Accountable institutions that are designated non-financial businesses and professions (DNFBPs) are urged to refer to public compliance communication (PCC) 53 for a detailed explanation on how an RMCP may be documented, including using a template that could aid in the documentation of an RMCP.

Supervisory approach

190AA. When conducting an inspection, the supervisory body may inspect whether the board of directors, senior management or person(s) with the highest authority approved the RMCP, in terms of section 42(2B) of the FIC Act.

190BB. The supervisory body will analyse and apply its mind to determine whether the accountable institution's board of directors, senior management or person(s) with the highest authority, understand the risks, which is translated into appropriate and adequate controls, including monitoring and oversight measures as part of the RMCP.

190CC. This is a holistic assessment of whether Part 1, Part 2 and Part 3 stated above have been covered in the accountable institution's RMCP, whether it has been described in the RMCP documentation, and whether the RMCP documentation (including reviews and amendments) has been approved by the board of directors, senior management or person(s) with the highest authority.

DRAFT

CHAPTER 5 IMPLEMENTATION OF THE UNITED NATIONS SECURITY COUNCIL RESOLUTIONS RELATING TO THE FREEZING OF ASSETS

191. The FIC Act places the responsibility to administer the targeted financial sanctions (TFS) measures adopted by the United Nations Security Council (UNSC) in its Resolutions on the Centre.

192. This inclusion of TFS measures is, inter alia, as a result of Recommendation 6 and 7 of the FATF recommendations, which requires member countries to implement the targeted financial sanctions proposed by the UNSC in the context of among other aspects, the prevention and suppression of terrorism and terrorist financing, as well as the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing and the relevant provisions of the FIC Act aim at enabling South Africa to meet these international obligations.

193. Sanctions impose restrictions on activities that relate to particular countries, goods and services, or persons and entities. TFS measures generally restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property. In order for these sanctions to be given effect, the FIC Act requires accountable institutions to freeze property and transactions pursuant to financial sanctions imposed in the UNSC Resolutions. Refer to the FIC public compliance communication 44A for further guidance on targeted financial sanctions.

Mechanisms for implementation

194. Mechanisms for the implementation of the UNSC Resolutions include the publication in the Government Gazette by the Minister of Finance of a Notice of the adoption of the UNSC Resolution, and the publication of a Notice by the Director of the Centre of persons who are subject to the sanction measures (the sanctions list). These Notices may be revoked if it is considered that they are no

longer necessary to give effect to the applicable UNSC Resolutions. Otherwise, the sanctions announced in these Notices remain in effect indefinitely.

195. The Notices by the Minister of Finance and the Director are public statements and are meant to advise both sanctioned persons and entities and accountable institutions who may have them as clients or prospective clients of the relevant sanctions. If an accountable institution has a sanctioned person or entity as a client, it is allowed to draw the attention of the person or entity to the relevant sanctions notices.

196. The acquisition, collection or use of the property of persons or an entity whose names appear in the sanctions is prohibited. This includes the provision of financial services and products to those persons or entities. In short this means that accountable institutions are not allowed to transact with a sanctioned person or entity or to process transactions for such a person or entity. The status quo as at the time of the imposition of the sanction in relation property or funds of the sanctioned person or entity must be maintained and no financial services may be provided to the person or entity. The only exception to this general prohibition is in specific instances where the Minister of Finance has permitted certain financial services or dealings with property as discussed below.

197. Accountable institutions must report to the Centre, the property in the accountable institution's possession or under its control which is owned or controlled by or on behalf of a person or an entity identified in the sanctions list.

Screening

198. Accountable institutions must be able to determine whether they have a sanctioned person or entity as a client or whether a prospective client is a sanctioned person or entity in order to determine their exposure to TFS-related obligations. This implies that accountable institutions which are likely to come into contact with

sanctioned persons or entities are able to screen clients and prospective clients against the relevant sanctions lists. This should be done during the client-take-on process as well as subsequently as and when the UNSC adopts new TFS measures or expand existing ones.

199. Accountable institutions must therefore determine the likelihood that their client base and intended target market may include sanctioned persons or entities. This should assist the accountable institution in determining the amount of effort and resources it requires in order to determine whether they have sanctioned persons or entities as a clients or whether prospective clients are sanctioned persons or entities. Accountable institutions that have business relationships with foreign persons and entities are more vulnerable to dealing with sanctioned persons and entities.

200. Accountable institutions should be mindful of the fact that failure to comply with TFS obligations is a criminal offence under section 49A of the FIC Act. The fact that an accountable institution had relied on a commercially available screening capability or that it had considered the risk of being exposed to TFS-related obligations to be low, would not be a defence against such a criminal charge.

Accessibility of sanctions list

201. The Centre will maintain an updated sanctions list which will be available on its website and which will reflect available identity particulars of persons and entities contained in notices published by the Director.

Basic living expenses

202. The FIC Act allows the Minister of Finance to permit a sanctioned person or entity to conduct financial services or deal with property affected by a sanction in order to allow such a person or entity access to certain basic living expenses. The permission of the Minister of Finance may contain the exact details of the types of

expenses which may be met from the property that is affected by a sanction, the amounts of such expenses, the funds or property from which such expenses may be met and the conditions to the access to the relevant funds or property.

203. The Minister of Finance may also permit the provision of financial services or the dealing in affected property which are not related to providing for basic living expenses, but which are necessary in the normal course of business e.g. allowing for the accrual of interest or other earnings or are necessary in order to avoid prejudice to third parties, e.g. contractual payments which predate the imposition of a sanction. As in the case of basic living expenses, the permission of the Minister of Finance may contain the exact details of the services, payments etc. that are permitted and the conditions thereto.

204. The permission of the Minister of Finance is granted by means of written communication with the sanctioned person or entity. The Director of the Centre must give notice of the permission of the Minister of Finance to accountable institutions and others who may have an interest therein. This is done by means of publishing notices containing the permission of the Minister of Finance and the conditions thereto on the Centre's website.

DRAFT

GLOSSARY

'Risk' means the impact and likelihood of ML/TF taking place. Risk refers to inherent risk, i.e. the level of risk that exists before mitigation. It does not refer to residual risk, i.e. the level of risk that remains after mitigation.

'**Risk factors'** means variables that, either on their own or in combination, may increase or decrease the ML/TF risk posed by a business relationship or single transaction.

'Risk-based approach' means an approach whereby accountable institutions identify, assess and understand the ML/TF risks to which institutions are exposed and take AML/CFT measures that are proportionate to those risks.

'Senior management' in an accountable institution is determined by the size, structure, and nature of the institution. The senior manager whose approval is sought for purposes of the FIC Act should have sufficient seniority and oversight to take informed decisions concerning the institution's compliance with the FIC Act that bind the institution to those decision.

'Source of funds' means the origin of the funds involved in a business relationship or single transaction. It includes both the activity that generated the funds used in the business relationship (for example the client's salary, occupation, business activities, proceeds of sale, corporate dividends, etc.), as well as the means through which the client's funds were transferred.

DRAFT

‘Source of wealth’ means the activities that have generated the total net worth of the client that is, the activities that produced the client’s funds and property (for example inheritance or savings).

End

Issued By:

THE DIRECTOR
FINANCIAL INTELLIGENCE CENTRE
12 June 2026

DRAFT