GUIDANCE AND RESOURCE DOCUMENT

for a

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

for Legal Practitioners Practising as Attorneys
(hereinafter referred to as 'this Document')

CONTENTS

IMPORTANT NOTICE AND DISCLAIMER

Please note that the Financial Intelligence Centre Act 38 of 2001 (FICA) requires an accountable institution to **develop, document, maintain and implement** a:

RISK MANAGEMENT AND COMPLIANCE PROGRAMME
(RMCP)

which must **enable** the accountable institution to identify, assess, monitor, mitigate and manage the risk that the provision by the accountable institution of new and existing products or services may involve or facilitate money laundering activities, terrorist financing and related activities or proliferation financing activities.

This means that:

1. **the adoption of a 'template/sample' RMCP is not envisaged under FICA**;
2. the adoption of an RMCP by itself does not constitute compliance with FICA, which requires the implementation of such a Programme; and
3. the accountable institution is required to, in addition to the adoption of the RMCP, identify, assess, monitor, mitigate and manage relevant risks in relation to individual client matters as well as to conduct a business-level risk assessment.

The RMCP should be unique to the particular Firm, having been prepared with due regard to the Firm's size, structure, service offering etc.

FICA provides that:

a. the board of directors, senior management or other person or group of persons exercising the highest level of authority in a Firm is required to approve the Firm's RMCP;
b. the Firm is required, in terms of Section 42(2C) of FICA, to review its RMCP at regular intervals to ensure that the RMCP remains relevant to its operations and the achievement of the requirements contemplated in Section 42(2);
c. the Firm is required to make documentation describing its RMCP available to all employees involved in transactions to which FICA applies; and
d. the Firm is required, on request, to make a copy of the documentation describing its RMCP available to the Financial Intelligence Centre (FIC).

The information contained in this Document is general in nature and cannot be interpreted or relied upon as legal advice.

Please note that the Financial Intelligence Centre (FIC) specifically expresses the view that guidance provided by it is authoritative in nature, which means that accountable institutions are required to take the guidance issued by the FIC into account in respect of their compliance with the relevant provisions of FICA and the Money Laundering and Terrorist Financing Control Regulations (MLTFCR/Regulations/Regulation).

Please further note that this Document takes into account amendments to FICA and related guidance up to **MAY 2025**.

ABBREVIATIONS/ACRONYMS

AML/CTF means anti-money laundering and counter-terrorist financing

AML/CTF/CPF means anti-money laundering, counter-terrorist financing and counter-proliferation financing

AI means accountable institution

CDD means Customer Due Diligence

Centre/FIC means the Financial Intelligence Centre established in terms of Section 2 of FICA

DNFBP means designated non-financial businesses and professions

DPEP means a domestic politically exposed person

EDD means Enhanced Due Diligence

FATF means the Financial Action Task Force

FICA means the Financial Intelligence Centre Act 38 of 2001

FPEP means a foreign politically exposed person

goAML means the IT system developed by UNODC for use by the FIC and other financial intelligence units

LPA means the Legal Practice Act 28 of 2014

LPC means the South African Legal Practice Council

LSSA means the Law Society of South Africa

ML means Money Laundering

MLTFCR/Regulations/Regulation means a reference to the Money Laundering and Terrorist Financing Control Regulations

PCC means a Public Compliance Communication issued by the FIC

PEP means a Politically Exposed Person

PF means Proliferation Financing

PIP means a Prominent Influential Person

POCA means the Prevention of Organised Crime Act 121 of 1998

POCDATARA Act means the Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004

RBA means a Risk-Based Approach

RCR means a Risk and Compliance Return

RMCP means a Risk Management and Compliance Programme as required in terms of Section 42 of FICA

SAR means a suspicious or unusual activity report in terms of Section 29 of FICA

SDD means Standard Due Diligence

SiDD means Simplified Due Diligence

STR means a suspicious or unusual transaction report in terms of Section 29 of FICA

TF means Terrorist Financing

TFAR means a terrorist financing activity report in terms of Section 29 of FICA

TFS means targeted financial sanctions

TFS List refers to the Targeted Financial Sanctions List pursuant to Section 26A of FICA

TFTR means a terrorist financing transaction report in terms of Section 29 of FICA

UNSC means the United Nations Security Council

INTRODUCTION TO AND OVERVIEW OF AN RMCP

1. INTRODUCTION

The RMCP is required in terms of FICA and will enable a law firm to comply with the law and to effectively address and mitigate the risk of money laundering and terrorist financing. The RMCP aims to make sure that all legal practitioners and employees of a firm know and can carry out the various steps included herein to identify clients, implement a risk-based approach (RBA) and apply the relevant legislation properly and satisfactorily.

RESOURCE:
The FIC has issued a *Reference Guide for All Accountable Institutions* to assist all new, and existing accountable institutions. It provides an overview of who the FIC is, what FICA requires from accountable institutions and directs accountable institutions to the range of issued guidance material that is available. The Reference Guide is available on the website of the FIC.
https://www.fic.gov.za/wp-content/uploads/2023/09/2022.12-CG-FIC-Act-reference-guide.pdf

2. GENERAL RESPONSIBILITIES IN TERMS OF FICA

All attorneys practising for their own account and as part of a commercial juristic entity contemplated in Sections 34(5)(a) and (b) of the Legal Practice Act 28 of 2014 (LPA) (referred to herein as a law firm/firm) are required to:

2.1 Register as an Accountable Institution

In terms of Section 43B of FICA, a law firm, as defined above, is required to:

a. register as an accountable institution (AI) with the Financial Intelligence Centre (FIC/Centre); and

b. notify the FIC in writing within 90 days of any changes to the particulars furnished to the Centre.

2.2 Provide Proof or Confirmation of Registration as an Accountable Institution

The South African Legal Practice Council (LPC) requires proof of registration in terms of FICA (i.e. the Org ID)[1] when registering a legal practice; attorneys are further required, in support of their applications for annual Fidelity Fund Certificates, to confirm in their Annual Statements on Trust Accounts that they are registered as AIs in terms of FICA.

2.3 Develop, Maintain and Implement a Risk Management and Compliance Programme

Section 42 of FICA provides that law firms are required to develop, document, maintain and implement an RMCP.

[1] According to FIC, an Org ID serves as the unique identifier for registrants. Once assigned an Org ID, further users from a firm can register for purposes of reporting on the goAML system.

An RMCP must enable a firm to identify, assess, monitor, mitigate and manage the risk that the provision by the firm of new and existing products or services may involve or facilitate money laundering (ML), terrorist financing (TF) or proliferation financing (PF).

2.4 Report to the Financial Intelligence Centre

A firm is required to submit certain reports to the FIC, which include reports in terms of Sections 28 and 29 of FICA, i.e. cash threshold reports and suspicious and unusual transaction reports.

2.5 Submit Risk and Compliance Return to the FIC

As per Directive 6 of 2023, law firms were required to submit a Risk and Compliance Return (RCR) to the FIC by 31 May 2023, which entailed the submission of information regarding their understanding of ML, TF and PF risks and their assessment of their compliance with their obligations in terms of FICA. **Very Important**: If a firm has not yet submitted its RCR it is still obligated to do so. Similar Directives may be issued in the future.

RESOURCE: The FIC has published Directive 6 of 2023.

2.6 Screening and Scrutinising of Current and Prospective Employees

As per Directive 8 of 2023, law firms are required to screen prospective employees and current employees for competence and integrity periodically, in a risk-based manner. Such employees are further required to be scrutinised against the targeted financial sanctions list (TFS List) referred to in Section 26A(3) of FICA.

RESOURCES: The FIC has published:
1. Directive 8 of 2023
2. Public Compliance Communication 55 on Directive 8, which provides guidance to accountable institutions on the application of Directive 8.

2.7 Duty to Keep Records

A firm is required to keep records of its compliance with its obligations under FICA, such as the information obtained during the performance of customer due diligence processes pertaining to its clients.

2.8 Training of Employees

A firm is required to ensure that regular training is offered to its employees (which includes its attorneys). Section 42(3) of FICA requires a firm to make its RMCP available to each of its employees involved in transactions to which FICA applies. Section 43 obliges a firm to provide ongoing training to its employees to enable them to comply with the provisions of FICA and the RMCP which are applicable to them.

3. THE PURPOSE OF THE RMCP

The RMCP will assist a firm to comply with its anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) obligations as well as its related professional conduct obligations.

The RMCP should enhance the capacity of a law firm to combat ML, TF and PF by providing a framework for the firm to implement effective controls and procedures. This includes performing due diligence on clients, monitoring transactions and reporting suspicious transactions. The effective implementation of these measures should reduce the risk of a firm being exposed to ML, TF or PF activities.

KEY FEATURES OF AN RMCP

1. RMCP GOVERNANCE

1.1 Accountability

The person/s exercising the highest level of authority in a firm should approve the RMCP and this should be indicated in the RMCP.

For example, the Sole Proprietor of [**APEX ATTORNEYS**] has approved this RMCP.

RESOURCES: The following sections and resources should be consulted:
1. Section 42 of FICA which is titled: **Risk Management and Compliance Programme**
2. Section 42A of FICA which is titled: **Governance of anti-money laundering, counter terrorist financing and financial sanction obligations compliance**
3. The FIC's Public Compliance Communication 53
4. The FIC's Guidance Note 7A

In the case of a commercial juristic entity, it would be indicated that the board of directors has approved the RMCP.

1.2 Date of Approval of the RMCP

The date upon which the RMCP was approved should be indicated in the RMCP (e.g. "This RMCP was approved on 2025/03/28").

1.3 Compliance Function

The persons responsible for the compliance function within a firm should be indicated in the RMCP.

For purposes of this Document, Section 34 of the LPA permits legal practitioners practising as attorneys to do so:

a. as a Sole Proprietor;
b. in a Partnership; or
c. as part of a Commercial Juristic Entity.

PCC 53 issued by the FIC provides that a firm is required to appoint a compliance officer and to be able to demonstrate that the compliance officer has sufficient competence and seniority to attend to the functions expected of a compliance officer.

The FIC indicates that the compliance officer can be named in the RMCP together with the level of competence and seniority that the compliance officer holds.

The duties of a compliance officer include:

a. drafting and reviewing the RMCP and ensuring compliance therewith;

b. ensuring compliance with the Customer Due Diligence (CDD) requirements and risk management systems;

c. ensuring the collection and retention of FICA-related documents and information and updates to client profiles; and

d. the approval of new or existing high-risk clients, which may require that approval be obtained from senior management in conjunction with the compliance officer before accepting a high-risk client and establishing a business relationship or concluding a single transaction.

PLEASE NOTE: Depending on the form of practice and the staff complement of a firm, senior management could consider, in addition to the appointment of a compliance officer, appointing a money laundering reporting officer to assist with the firm's FICA reporting obligations and to assist senior management in meeting their compliance obligations.

[Where applicable] Branch Implementation:

FICA requires that a firm ensures, where applicable, that the RMCP is implemented in the firm's branches and, should the firm not have any branches, this should be indicated in the RMCP, as provided for in Section 42(2A), read with Section 42(2)(q), of FICA.

1.4 Registration as an Accountable Institution

A firm is required to register as an AI with the FIC via its goAML registration and reporting platform. This registration should be confirmed in the RMCP, along with the firm's registration reference number.

RESOURCE: The following resource should be consulted:
The FIC's goAML Registration Guideline for Accountable and Reporting Institutions

1.5 Review of the RMCP

It is important for the RMCP to be reviewed annually by a firm to ensure that it remains up-to-date and effective in identifying, assessing and mitigating risks. Regular review of the RMCP allows a law firm to effect necessary updates and changes to reflect the current regulatory environment, industry best practices, and a firm's own risk profile.

A firm should also review the RMCP regularly as ML/TF/PF risks can change over time. New challenges and weaknesses may appear, and the rules may vary. By reviewing the RMCP annually or earlier when legislative or other relevant changes take place, a firm can, where applicable, make necessary updates and changes to reflect the current risk environment and maintain the effectiveness of its risk management and compliance processes.

The revision process can be recorded in the RMCP in a schedule format.

2. A FIRM'S RISK-BASED APPROACH

An RBA, according to the Financial Action Task Force (FATF), is a method via which legal professionals assess and manage the risks of ML and TF based on the specific circumstances of each client and transaction. It involves identifying potential risks, evaluating their severity, and applying appropriate measures to mitigate them, ensuring that resources are focused on higher-risk areas.

The RBA allows a firm to allocate its resources more efficiently by focusing on higher-risk clients and transactions, thereby enhancing the effectiveness of their AML/CTF/CPF efforts. It also assists in building a more robust compliance framework, reducing the likelihood of legal and reputational risks associated with non-compliance.

The rationale behind the RBA is to ensure that the measures taken to prevent ML/TF/PF risks from materialising are proportionate to the risks identified, making the process more efficient and targeted.

By understanding and addressing the ML/TF/PF risks associated with different clients and transactions, a firm can better protect itself and the financial system from abuse.

2.1 Benefits of the RBA:

a. **Optimal Resource Distribution**: An RBA will enable a firm to prioritise its resources on higher risk clients and transactions, enhancing its AML/CTF/CPF performance and productivity.

b. **Improved Compliance**: A firm can strengthen its compliance framework by using an RBA, lowering the likelihood of legal and reputational risks that come with non-compliance.

c. **Tailored Measures**: An RBA allows a firm to apply measures that are specifically tailored to the risks identified, ensuring that the actions taken are proportionate and relevant to the specific circumstances.

d. **Better Risk Management**: A firm can more effectively identify and handle the risks of different clients and transactions, guarding itself and the financial system against possible misuse.

e. **Regulatory Compliance**: An RBA assists a firm to comply with regulatory standards by identifying and mitigating risks efficiently, which is vital to maintaining trust and credibility in the legal profession.

2.2 Examples of unique characteristics:

These unique characteristics should be considered in a firm's RBA:

a. **Client Attributes**: A client's industry and geographic location can influence a risk assessment significantly, especially if he/she/it operates in high-risk regions or jurisdictions.

b. **Risk Assessment Capabilities**: Law firms vary in their ability to conduct risk assessments based on their size and resources, with smaller firms typically using public information and larger firms having more resources for comprehensive checks.

c. **Nature of Services Provided**: The specific services offered by law firms, such as conveyancing transactions or managing client assets, can be more susceptible to ML/TF/PF risks.

d. **Complexity of Transactions**: Unusual complexity in control or ownership structures of a client or a transaction without clear explanation can be a red flag, requiring a more detailed risk assessment and due diligence.

e. **Client Behaviour**: Clients who offer to pay unusually high fees for services that do not typically warrant such premiums may pose higher risks and require enhanced due diligence.

3. THE FIRM'S BUSINESS-LEVEL RISK ASSESSMENT

The FIC requires that all firms conduct a business-level risk assessment. A business-level risk assessment is important for several reasons, specifically:

3.1 Identification of Risks:

It aids in identifying potential risks a firm may face in the context of ML/TF/PF. Understanding these risks is crucial to developing strategies to mitigate said risks.

3.2 Avoiding ML/TF/PF:

The assessment is a key step to preventing a firm from being abused for ML/TF/PF purposes. An assessment can assist a firm to ascertain the risks of being exposed to the proceeds of financial crime and to set up suitable policies, controls and procedures to reduce these risks.

3.3 Protecting Integrity and Reputation:

A good business-level risk assessment is key to a firm's integrity and reputation as it would enable the firm to avoid negative publicity associated with potential clients associated with illicit activities.

3.4 Operational Efficiency:

By understanding the ML/TF/PF risks, a firm is able to re-direct its resources to address the higher risk areas, thereby maximising the efficient application of its resources.

3.5 Client Trust:

A firm handles sensitive information and assists clients to comply with the law. By carrying out a comprehensive risk assessment, a firm demonstrates to clients that it is committed to meeting its compliance obligations, which ultimately builds trust in client relationships.

3.6 Training and Awareness:

It identifies where training is needed.

3.7 Flexibility:

A risk assessment at the business level assists a firm to remain flexible and to react promptly to shifts in the risk environment.

Conducting a business-level risk assessment is essential for the running of a compliant law firm. It assists a firm to comply with rules and to mitigate risks, as well as to make informed choices and thereby maintain its reputation as a responsible firm. The business-level risk assessment should be preceded by the firm's review of the following:

a. The South African National Terrorism Financing Risk Assessments of 31 March 2022 and the updated version published in June 2024. The risk assessments focus on, *inter alia,* the threats, vulnerabilities and possible impact of terror financing on South Africa's safety and stability.

b. The Assessments of the Inherent Money Laundering and Terrorist Financing Risks: Legal Practitioners of March 2022 and March 2024. The risk assessments focus on the legal practitioners' sector. A firm should be mindful of relevant assessments and the FIC's website should be visited regularly to determine whether existing assessments have been updated or further assessments published. The above assessments should serve to inform the firm's risk-based approach and business-level risk assessment.

RESOURCES: The following resources should be consulted:

The FIC has published Guidance Note 7A – Implementation of various aspects of the FIC Act, which is available at: https://www.fic.gov.za/wp-content/uploads/2025/02/2025.2-GN-implementation-of-fic-act.pdf

BUSINESS-LEVEL RISK ASSESSMENT

Please note that the below offers an example of the potential content of a business-level risk assessment, subject to the specific characteristics of the firm (i.e. small, large, specialist, etc.). This assessment should inform the firm's RMCP.

IMPORTANT: The items listed below are not meant to be prescriptive or to provide an exhaustive list of indicators or characteristics and should be amended or expanded upon as required within the firm's particular context.

COUNTRY OR GEOGRAPHIC RISK		
Potential Factors applicable to country/jurisdiction:	**Applicability**	**RATING**
Countries with high-risk jurisdictions known for weak AML/CTF/CPF controls, high levels of corruption, or subject to international sanctions.	APPLICABLE	Choose an item.
Countries identified by FATF as high-risk or non-cooperative jurisdictions or that have not implemented the recommendations of international bodies like FATF.	APPLICABLE	Choose an item.
Countries with high levels of corruption, as indicated by indices such as Transparency International's Corruption Perceptions Index	APPLICABLE	Choose an item.
Countries with ineffective legal systems, lack of judicial independence, or slow judicial processes	APPLICABLE	Choose an item.
RATING – COUNTRY OR GEOGRAPHIC RISK	Choose an item.	

SERVICE OR TRANSACTION RISK		
Potential Factors applicable to service/transaction risk:	**Applicability**	**RATING**
Services involving multiple jurisdictions, intricate financial structures, or layered transactions.	APPLICABLE	Choose an item.
High monetary value transactions or services (e.g., large property deals, significant corporate transactions).	APPLICABLE	Choose an item.
Services that can be used to obscure ownership or source of funds (e.g., trust and company formation, offshore services).	APPLICABLE	Choose an item.
Regular or high-volume transactions that could indicate layering or structuring.	APPLICABLE	Choose an item.
RATING – SERVICE OR TRANSACTION RISK	Choose an item.	

CLIENT RISK

Potential Factors applicable to client risk:	Applicability	RATING
Unusual or complex transaction patterns, high volume of transactions inconsistent with the client's known profile, or transactions just below reporting thresholds.	APPLICABLE	Choose an item.
Client with adverse media coverage, known associations with criminal activities, or previous involvement in regulatory breaches.	APPLICABLE	Choose an item.
Clients with a history of legal issues, frequent litigation, or regulatory sanctions.	APPLICABLE	Choose an item.
Client's source of wealth and funds or business partners originating from high-risk industries, jurisdictions, or lacking clear provenance.	APPLICABLE	Choose an item.
Conducting business with foreign politically exposed persons (FPEPs) and those closely associated with or related to FPEPs.	APPLICABLE	Choose an item.
RATING – CLIENT RISK	Choose an item.	

BUSINESS CHANNELS		
Potential Factors applicable to business channels:	**Applicability**	**RATING**
Predominantly non-face-to-face onboarding, reliance on third-party introductions without thorough verification.	APPLICABLE	Choose an item.
Widespread use of intermediaries or agents, especially in higher risk areas or without adequate due diligence.	APPLICABLE	Choose an item.
Business models involving anonymous or complex delivery channels.	APPLICABLE	Choose an item.
Payment methods with high risk (e.g., cash, cryptocurrencies) and complex transaction processing systems.	APPLICABLE	Choose an item.
Working with third-party service providers from high-risk areas or with poor AML/CTF/CPF controls.	APPLICABLE	Choose an item.
Use of unsecured or anonymous communication channels (e.g., encrypted messaging apps, non-company email addresses).	APPLICABLE	Choose an item.
RATING – BUSINESS CHANNELS	Choose an item.	
COMBINED TOTAL OF RISK-RATING (NEW SERVICES)		
IF APPLICABLE, COMMENTS:		

COMBINED TOTAL OF RISK-RATING

Business Level Assessment: The overall Business Level Risk Assessment of the firm is: [Choose an item.]
IF APPLICABLE, COMMENTS:

4. A FIRM'S ASSESSMENT OF NEW SERVICES

Trust and credibility are essential to a firm and failing to manage ML/TF/PF risks when offering new services can harm its reputation, resulting in a loss of clients and future business opportunities. A firm also has a fiduciary duty to safeguard its clients' interests, this includes ensuring that its services are not misused for illegal activities.

Risk assessments in respect of new services will help detect and reduce potential ML/TF/PF risks. By incorporating risk assessments into the development of new services, a firm can innovate confidently, knowing that it is compliant with regulations and protected against potential risks.

In doing so, a firm will:

4.1 identify possible ML/TF/PF risks that may arise from new services;

4.2 evaluate the probability and consequence of identified ML/TF/PF risks;

4.3 establish and execute strategies to reduce identified ML/TF/PF risks; and

4.4 monitor the performance of risk reduction strategies and update them periodically to ensure that they are still effective in the changing regulatory environment.

Such an assessment would only be required in circumstances where a firm intends offering new services, i.e. services that have not previously been risk-assessed.

The assessment on the following pages contains criteria that may be applicable in conducting a risk assessment of new services and will be dependent on whether the firm, at the time of carrying out the assessment, has determined the client target market, geographic location and method of delivery.

Such a risk assessment would be incorporated into the periodic business-level risk assessment reviews.

ASSESSMENT OF NEW SERVICES

TO DETERMINE THE POTENTIAL ML/TF/PF RISKS OF NEW SERVICES

Please note that the below offers an example of the potential content of a risk assessment for new services to be rendered by a firm, subject to the specific characteristics of the firm (i.e. small, large, specialist, etc.). This assessment should inform the firm's RMCP.

Creating a risk matrix for a law firm in compliance with FICA and Public Compliance Communication (PCC) 53 involves assessing various risk criteria as identified by FATF. This risk assessment is focused on an assessment of new services, not on individual clients, and takes into account the following key risk criteria:

COUNTRY OR GEOGRAPHIC RISK		
Potential Factors applicable to country/jurisdiction:	**Applicability**	**RATING**
High-risk countries or jurisdictions known for weak AML/CTF/CPF controls, high levels of corruption, or subject to international sanctions.	APPLICABLE	Choose an item.
Countries identified by FATF as high-risk or non-cooperative jurisdictions or that have not implemented the recommendations of international bodies like FATF.	APPLICABLE	Choose an item.
Countries with ineffective legal systems, lack of judicial independence, or slow judicial processes.	APPLICABLE	Choose an item.
RATING – COUNTRY OR GEOGRAPHIC RISK	Choose an item.	

SERVICE OR TRANSACTION RISK		
Potential Factors applicable to service/transaction risk:	**Applicability**	**RATING**
Services involving multiple jurisdictions, intricate financial structures, or layered transactions.	APPLICABLE	Choose an item.
High monetary value transactions or services (e.g., large property deals, significant corporate transactions) or high-volume transactions that could indicate layering or structuring.	APPLICABLE	Choose an item.
Services that can be used to obscure ownership or source of funds (e.g., trust and company formation, offshore services).	APPLICABLE	Choose an item.
RATING – SERVICE OR TRANSACTION RISK	Choose an item.	

CLIENT RISK		
Potential Factors applicable to client risk:	**Applicability**	**RATING**
Client's source of wealth and funds or business partners originating from high-risk industries, jurisdictions, or lacking clear provenance.	APPLICABLE	Choose an item.
Conducting business with foreign politically exposed persons (FPEPs) and those closely associated with or related to FPEPs.	APPLICABLE	Choose an item.

RATING – CLIENT RISK	Choose an item.	
BUSINESS CHANNELS		
Potential Factors applicable to business channels:	**Applicability**	**RATING**
Predominantly non-face-to-face or anonymous communication channels for onboarding.	APPLICABLE	Choose an item.
Payment methods with high risk (e.g., cash, cryptocurrencies) and complex transaction processing systems.	APPLICABLE	Choose an item.
Working with third-party service providers or intermediaries or agents from high-risk areas or with poor AML/CTF/CPF controls.	APPLICABLE	Choose an item.
RATING – BUSINESS CHANNELS	Choose an item.	
COMBINED TOTAL OF RISK-RATING (NEW SERVICES)		
IF APPLICABLE, COMMENTS:		

COMBINED TOTAL OF RISK-RATING
New Services Assessment: The new services Risk Assessment of the firm is: [Choose an item.]
IF APPLICABLE, COMMENTS:

5. A FIRM'S CLIENT-LEVEL RISK ASSESSMENT

A firm should use a systematic approach to assessing the risk level of each client. This would involve examining various factors such as client profiles, products or services offered, business channels and geographic locations. Each factor should be evaluated based on specific features that indicate the risk level, and suitable client verification measures to mitigate the risk.

In summary, a firm should use a systematic risk assessment approach, taking into account client profiles, products or services, business channels and geographic locations, to comply with AML/CTF/CPF requirements. By recognising and classifying risks, a firm will be able to implement suitable verification measures, ensuring strong risk management and regulatory compliance.

CLIENT-LEVEL RISK ASSESSMENT

INDICATING THE ML/TF/PF RISKS

THAT BUSINESS RELATIONSHIPS OR SINGLE TRANSACTIONS POSE

Please note that the below offers an example of the potential indicators and characteristics that could be taken into account when conducting client-level risk assessments.

INDICATOR	CHARACTERISTIC	APPLICABILITY	RISK-RATING SCORE
Country or Geographic Location Onboarding	Clients located in or conducting business with high-risk jurisdictions known for weak AML/CTF/CPF controls, high levels of corruption, or subject to international sanctions	APPLICABLE	**LOW**
	Clients located in jurisdictions with strong AML/CTF/CPF controls and low levels of corruption	APPLICABLE	
Country or Geographic Location Onboarding	Countries identified by FATF as high-risk or non-cooperative jurisdictions.	APPLICABLE	**LOW**
	Countries that are FATF member states with robust compliance records.	APPLICABLE	
Country or Geographic Location Onboarding.	Countries with high levels of corruption, as indicated by indices such as Transparency International's Corruption Perceptions Index.	APPLICABLE	**LOW**
	Countries with low levels of corruption and strong anti-corruption measures.	APPLICABLE	
Country or Geographic Location Onboarding	Jurisdictions with ineffective legal systems, lack of judicial independence, or slow judicial processes.	APPLICABLE	**LOW**
	Jurisdictions with efficient legal systems, independent judiciary, and timely legal processes.	APPLICABLE	

Country or Geographic Location Onboarding	Countries that do not cooperate with international AML/CTF/CPF efforts, or that have not implemented the recommendations of international bodies like FATF.	APPLICABLE	**LOW**
	Countries that actively participate in international AML/CTF/CPF initiatives and fully implement FATF recommendations.	APPLICABLE	
Country or Geographic Location Onboarding	Countries that are uncooperative in providing beneficial ownership information to authorities.	APPLICABLE	**LOW**
	Countries that are cooperative in providing beneficial ownership information to authorities.	APPLICABLE	
Service Onboarding	Services involving multiple jurisdictions, intricate financial structures, or layered transactions.	APPLICABLE	**LOW**
	Simple, straightforward transactions (e.g., drafting a will, local real estate transactions).	APPLICABLE	
Service Onboarding	Regular or high-volume transactions that could indicate layering or structuring.	APPLICABLE	**LOW**
Service Onboarding & Ongoing	High monetary value transactions or services (e.g., large property deals, significant corporate transactions).	APPLICABLE	**LOW**
	Low monetary value transactions or services (e.g., basic legal advice, small claims).	APPLICABLE	
Service Onboarding & Ongoing	Services that can be used to obscure ownership or source of funds (e.g., trust and company formation, offshore services).	APPLICABLE	**LOW**
	Routine legal services with minimal risk of abuse for money laundering or terrorist financing.	APPLICABLE	
	Infrequent or one-off transactions.	APPLICABLE	
Service Onboarding & Ongoing	Use of cash, cryptocurrencies, or other non-traceable payment methods.	APPLICABLE	**LOW**
Client Onboarding	Client with adverse media coverage, known associations with criminal activities, or previous involvement in regulatory breaches.	APPLICABLE	**LOW**
	Client with a positive reputation, no adverse media coverage, and no history of regulatory breaches.	APPLICABLE	
Client Onboarding	Clients with a history of legal issues, frequent litigation, or regulatory sanctions.	APPLICABLE	**LOW**

	Clients with no significant legal issues or regulatory sanctions.	APPLICABLE	
Client Onboarding & Ongoing	Wealth or funds originating from high-risk industries, jurisdictions, or lacking clear provenance.	APPLICABLE	**LOW**
	Wealth or funds from verified, legitimate sources such as salaries, business profits, or investments from reputable institutions.	APPLICABLE	
Client Onboarding & Ongoing	Clients with business partners or associates from high-risk jurisdictions or industries, or with opaque relationships.	APPLICABLE	**LOW**
	Clients with transparent, well-documented business relationships in low-risk jurisdictions and industries.	APPLICABLE	
Client Ongoing	Unusual or complex transaction patterns, high volume of transactions inconsistent with the client's known profile, or transactions just below reporting thresholds.	APPLICABLE	**LOW**
	Normal, predictable transaction patterns consistent with the client's known profile and business activities.	APPLICABLE	
	Use of traceable and regulated payment methods (e.g., bank transfers, credit card payments).	APPLICABLE	
Business Channels Onboarding	Predominantly non-face-to-face onboarding (e.g., online, email), reliance on third-party introductions without thorough verification.	APPLICABLE	**LOW**
	Direct face-to-face onboarding with thorough CDD procedures, in-person meetings.	APPLICABLE	
Business Channels Ongoing.	Heavy reliance on intermediaries or agents, especially those in high-risk jurisdictions or without proper due diligence.	APPLICABLE	**LOW**
	Minimal use of intermediaries, or use of reputable, well-known intermediaries with strong compliance frameworks.	APPLICABLE	
Business Channels Ongoing	Business models involving anonymous or complex delivery channels.	APPLICABLE	**LOW**
	Traditional business models with clear and transparent delivery channels.	APPLICABLE	
Business Channels Ongoing	Use of high-risk payment methods (e.g., cash, cryptocurrencies), complex transaction processing systems.	APPLICABLE	**LOW**

	Use of regulated and traceable payment methods (e.g., bank transfers, credit card payments), straightforward transaction processing.	APPLICABLE	
Business Channels Ongoing.	Use of unsecured or anonymous communication channels (e.g., encrypted messaging apps, non-company email addresses).	APPLICABLE	**LOW**
	Use of secure, company-controlled communication channels (e.g., company email, secure client portals).	APPLICABLE	
Other factors Ongoing	Outdated or poorly implemented internal systems, lack of regular reviews and updates.	APPLICABLE	**LOW**
	Up-to-date, well-implemented internal systems, regular reviews and updates.	APPLICABLE	
Other factors Ongoing	Infrequent or inadequate training on AML/CTF/CPF and compliance issues.	APPLICABLE	**LOW**
	Regular, comprehensive training programmes on AML/CTF/CPF and compliance issues.	APPLICABLE	

Depending on a client's risk-rating the firm would adopt one of the following client identification and verification measures provided for in paragraphs 5.1 to 5.3 below:

5.1 Simplified Due Diligence (SiDD)

SiDD is usually applied for low-risk clients. The firm should list in its RMCP the information, documentation and/or electronic records that it should obtain from a client when carrying out SiDD.

5.2 Standard Due Diligence (SDD)

SDD is usually applied for medium-risk clients. The firm should list in its RMCP the information, documentation and/or electronic records that it should obtain from a client when carrying out SDD.

5.3 Enhanced Due Diligence (EDD)

EDD is usually required to be applied for high-risk single transactions and business relationships. The firm should list in its RMCP the information, documentation and/or electronic records that it should obtain from a client when carrying out EDD. The FIC provides that, in such circumstances, the firm's systems and controls should provide for more information to be obtained about their clients, applying more secure methods to confirm client information, and closely monitoring clients' transaction activities.

It should also be noted that FICA specifically requires the implementation of the following forms of further due diligence in the specific circumstances:

5.4 Additional Due Diligence (ADD)

ADD is applied in respect of clients that are legal persons, trusts or partnerships, as stipulated under Section 21B of FICA. ADD includes establishing the nature of the client's business, establishing the ownership and control structure of the client and identifying the beneficial owner of the client.

5.5 Ongoing Due Diligence (ODD)

ODD is conducted in respect of clients in a business relationship with the intervals at which CDD is updated/repeated (which forms part of the ODD process) being determined by the risk-rating allocated to the client, as stipulated under Section 21C of FICA. The ODD process includes the monitoring of transactions throughout the course of the relationship, which includes the source of funds and relevant background information. For instance, CDD could be updated/repeated annually for high-risk clients, every two years for medium-risk clients, and every three years for low-risk clients. There are other instances in which CDD may be updated/repeated, such as where a change in a client's transaction pattern is detected or where a suspicious transaction report is filed in respect of the client. The firm should list in its RMCP the information, documentation and/or electronic records that it should request when carrying out the ODD process.

6. OVERVIEW OF THE POTENTIAL ATTORNEY AND CLIENT RELATIONSHIP

A firm should, before entering into a professional relationship with a prospective client, determine whether the prospective client would be entering into a single transaction or a business relationship.

6.1 Important concepts

In order to make this determination, a firm should understand the definitions of the concepts client, single transaction and business relationship. FICA defines these concepts as follows:

a. A "**business relationship**" means an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis;

b. A "**single transaction**" refers to a transaction (a) other than a transaction concluded in the course of a business relationship; and (b) where the value of the transaction is not less than the amount prescribed[2], except in the case of Section 20A (anonymous client); and

c. A "**client**" means a person who has entered into a business relationship or a single transaction with an AI.

[2] At the date of publication, the amount prescribed is an amount of not less than R5 000,00. It is imperative to establish the applicable prescribed amount.

6.2 Anonymous client or person with an apparent false or fictitious name

It should be noted that Section 20A of FICA prohibits a firm from establishing a business relationship or concluding a single transaction with an anonymous client or a client with an apparent false or fictitious name. This prohibition also applies to transactions that are less than the amount prescribed, as discussed below. The manner in which a firm complies with this requirement, both below and above the threshold, should be recorded in the RMCP. A firm is not permitted to accept instructions from an anonymous client or a client with an apparent false or fictitious name.

6.3 Transactions less than the prescribed amount

A firm is not required to carry out the full scope of CDD measures where the value of the transaction is less than the amount prescribed (i.e. R5 000 at time of publication). A firm should, however, in such instances, obtain and record at least sufficient information describing the identity of the client. The FIC offers, as an example of the information that should be obtained, the full name and identity number of the client and other information such as a contact number. This client is also required to be scrutinised against the TFS list. The FIC does, however, further suggest the added step of viewing the identification document of the client.

6.4 Identification of clients and other persons

Section 21(1) provides that when a firm engages with a prospective client to enter into a single transaction or to establish a business relationship, a firm is required to, in the course of concluding that single transaction or establishing that business relationship and in accordance with its RMCP:

a. establish and verify the identity of the client;

b. if the client is acting on behalf of another person, establish and verify:

   (i) the identity of that other person; and
   (ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and

c. if another person is acting on behalf of the client, establish and verify:

   (i) the identity of that other person; and
   (ii) that other person's authority to act on behalf of the client.

6.5 Understanding and obtaining information on a business relationship

Section 21A requires a firm, when engaging with a prospective client to establish a business relationship, to also obtain information to reasonably enable a firm to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with a firm's knowledge of that prospective client, including information describing:

a. the nature of the business relationship concerned;

b. the intended purpose of the business relationship concerned; and

c. the source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship concerned.

6.6 Domestic Politically Exposed Persons and Prominent Influential Persons

A firm is required to determine whether a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a **domestic politically exposed person (DPEP)** or a **prominent influential person** (**PIP**) as listed in Schedules 3A and 3C. The same requirements apply in the event of immediate family members and known close associates of DPEPs and PIPs.

6.7 Foreign Politically Exposed Persons

A similar process, as set out for a DPEP or a PIP, is required to be adopted in relation to a foreign politically exposed person (FPEP), as listed under Schedule 3B of FICA. The same requirements apply in the event of immediate family members and known close associates of FPEPs.

6.8 Beneficial Owners

A firm is required to establish the identity of the beneficial owners of clients that are legal persons, trusts and partnerships and to take reasonable steps to verify their identities as provided for in this document.

7. CLIENT IDENTIFICATION – INDIVIDUALS

A firm should consider the following in endeavouring to comply with the identification and verification requirements of individual clients:

7.1 Client Identification and Verification:

a. **Obtain detailed information**: Full name, date of birth, residential address, contact information, and identification number.

b. **Verify identity**: Obtain and verify via an official identification document, such as a South African identity document (ID), passport, or driver's license.

c. **Address verification**: Obtain proof of a residential address through documents such as utility bills, bank statements, or lease agreements.

7.2 Record Keeping:

Maintain documentation: Keep a copy of the identification documents and records of information obtained during the verification process.

Retain records: Ensure that records are kept for at least five years from the date of termination of the business relationship or from the conclusion of a single transaction.

8. CLIENT IDENTIFICATION – LEGAL PERSONS, PARTNERSHIPS & TRUSTS

FICA identifies a legal person as any person, other than a natural person, that establishes a business relationship or enters into a single transaction with an AI and includes a person incorporated as a company, a close corporation, a foreign company or any other form of corporate arrangement or association, but excludes a trust, a partnership or a sole proprietor. Section 21B(1) of FICA requires that where a prospective or existing client is a legal person or a natural person acting on behalf of a partnership, trust or similar arrangement between natural persons, a firm is required to establish:

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

A firm should therefore endeavour to request and obtain information on the ownership and control structure of its clients, to understand its clients' ownership and control structure and to take reasonable steps to verify the ownership and control structure information obtained.

A firm should also understand the different types, forms and basic features of legal persons, trusts or partnerships onboarded as its clients or potential clients. A firm is required to identify a legal person, trust or partnership, and the person(s) acting on behalf of a legal person, trust or partnership, as well as its beneficial owner/s.

A firm should consider taking the following steps in endeavouring to comply with the identification and verification requirements in relation to a legal person, trust or partnership. The specific legal records/documents available to meet these requirements will be dealt with in more detail below:

a. identify the legal name of the entity;
b. request the official registration number of the legal entity;
c. collect information on the type of legal entity (e.g., corporation, partnership, or trust);
d. request copies of official registration documents, such as a memorandum of incorporation or a trust deed;
e. identify and verify the identities of directors, trustees, or other authorised persons within the legal entity;
f. verify the physical address of the legal entity;
g. keep detailed records of the identification process and ongoing monitoring of the legal entity;
h. conduct periodic reviews and updates of the client's information to ensure continued compliance with regulatory requirements.

8.1 Collection of Documentation and Information to Establish:

a. Legal Name:

- registration certificate;
- letters of authority;
- partnership agreement;
- memorandum of incorporation;
- trust deed;
- letterhead; and
- business invoice.

b. Address and other Relevant Particulars:

- Proof of registered and/or physical address and, where applicable, notice of change of address;
- Telephone number;
- Registration certificate, letters of authority, NPO certificate, etc.; and
- The Identification and Verification of the natural persons authorised to give instructions to a firm on behalf of the entity.

c. An Understanding and Obtaining Information Concerning a Business Relationship

A firm is required, when entering into a business relationship, to obtain information to reasonably enable a firm to determine whether future transactions that will be performed are consistent with a firm's knowledge of that prospective client, including information describing:

- the nature of the business relationship concerned;
- the intended purpose of the business relationship concerned; and
- the source of the funds which that prospective client expects to use in concluding transactions in the course of the business relationship concerned.

8.2 Additional Due Diligence Measures Relating to Legal Persons, Partnerships, Trusts, other Similar Arrangements

The following additional due diligence measures could be considered in relation to legal persons, partnerships, trusts or other similar arrangements, whether they originated or were incorporated in South Africa or beyond:

a. Legal Status Verification:

- Confirm a company's legal status and registration on the website of the Companies and Intellectual Property Commission (CIPC);
- Confirm a Trust's legal status on the ICMS website of the Master's office;
- Confirm the registration status of an NPO on the website of the NPO Directorate.

b. Organisational Structure:

- Review a company's memorandum of incorporation;
- Review a trust's trust deed;
- Review an NPO's founding document;
- Review a partnership's partnership agreement.

c. **Directors and Officers:**
   - Obtain a list of current and, where applicable, past directors, trustees, board members, partners and officers;
   - If required, conduct background checks and verify the qualifications of key management personnel.

d. **Identifying a legal person's representative:**
   Determine whether a client is a legal person, partnership or trust or a natural person acting on behalf of a legal person, partnership or trust.

9. WHAT IS A BENEFICIAL OWNER?

RESOURCE: The FIC has published **PCC 59** - Relating to beneficial ownership and the application of Section 21B of the Financial Intelligence Centre Act
https://www.fic.gov.za/wp-content/uploads/2024/08/PCC-59-Beneficial-ownership.pdf

FICA defines a beneficial owner as a natural person who directly or indirectly – (i) ultimately owns or exercises effective control of – (aa) a client of an AI; or (bb) a legal person, partnership or trust that owns or exercises effective control of, as the case may be, a client of an AI; or (ii) exercises control of a client of an AI on whose behalf a transaction is being conducted; and (b) includes – (i) in respect of legal persons, each natural person contemplated in Section 21B(2)(a); (ii) in respect of a partnership, each natural person contemplated in Section 21B(3)(b); and (iii) in respect of a trust, each natural person contemplated in Section 21B(4)(c), (d) and (e).

Where a prospective or existing client is a legal person, a firm is required to identify the natural person who is the beneficial owner of the client, as provided for in Section 21B of FICA. Where a firm fails to identify such a natural person, the requirement as set out in Section 21B of FICA will not have been met.

Identifying the natural person(s) who are the beneficial owner(s) provides the required understanding as to who ultimately receives the benefits from a client.

Important: A firm should recognise, understand and draw a distinction between a beneficial owner and a legal owner. The legal owner may not always be the beneficial owner.

The concept of beneficial owner is widely defined and a person having a controlling ownership interest would include a person(s) having the power to, for example:
- dispose of or control the legal entity's property;
- amend or terminate the legal entity;
- remove or add board members, shareholders or beneficiaries or to give another individual control over the legal entity; or
- veto specified decisions or resolutions.

PCC 59 mentions that trends show that criminals often abuse legal persons, trusts and partnerships to obscure the ownership or control of funds derived from illegal activities. This, it is said, is achieved by the creation of different levels of ownership which, in turn, makes it difficult to identify the ultimate beneficial owner of the legal person, trust or partnership. It is therefore

important that a firm identifies the natural person/s who own or control clients that are legal persons, trusts or partnerships.

As part of the CDD process referred to above, where clients are legal persons, trusts or partnerships, a firm is required to ascertain the ownership and control structure of the client. Establishing and understanding the ownership and control structure of a client will assist a firm in complying with Section 21B, which requires that a firm identify all natural persons who are the beneficial owner/s of the client.

Section 21B(2) of FICA provides the key requirements for the identification and verification of the beneficial owners of legal persons.

Section 21B(2) provides as follows:

> If a client contemplated in Section 21 is a legal person, an accountable institution must, in addition to the steps required under Sections 21 and 21A and in accordance with its Risk Management and Compliance Programme –
>
> (a) establish the identity of the beneficial owner of the client by:
>
> (i) determining the identity of each natural person who, independently or together with another person, has a controlling ownership interest in the legal person;
>
> (ii) if in doubt whether a natural person contemplated in subparagraph (i) is the beneficial owner of the legal person or no natural person has a controlling ownership interest in the legal person, determining the identity of each natural person who exercises control of that legal person through other means, including through his or her ownership or control of other legal persons, partnerships or trusts; or
>
> (iii) if a natural person is not identified as contemplated in subparagraph (ii), determining the identity of each natural person who otherwise exercises control over the management of the legal person, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director or manager; and
>
> (b) take reasonable steps to verify the identity of the beneficial owner of the client, so that the accountable institution is satisfied that it knows who the beneficial owner is.

It is evident from the above extract of FICA that a firm is required to:

- establish the identity of the beneficial owner/s of a client that is a legal person;
- take reasonable steps to verify the identity of the beneficial owner/s;
- ensure that its RMCP makes provision for the identification and verification of the said beneficial owners.

FICA defines a beneficial owner as follows:

> "Beneficial owner" –
> (a) means a natural person who directly or indirectly:
>
> (i) ultimately owns or exercises effective control of –
>
> (aa) a client of an accountable institution; or
> (bb) a legal person, partnership or trust that owns or exercises effective control of, as the case may be, a client of an accountable institution; or
>
> (ii) exercises control of a client of an accountable institution on whose behalf a transaction is being conducted; and
>
> (b) includes:
>
> (i) in respect of legal persons, each natural person contemplated in Section 21B(2)(a);
>
> (ii) in respect of a partnership, each natural person contemplated in Section 21B(3)(b); and
>
> (iii) in respect of a trust, each natural person contemplated in Section 21B(4)(c), (d) and (e).

10. DETERMINING THE BENEFICIAL OWNER OF LEGAL PERSONS, PARTNERSHIPS AND TRUSTS

In determining the beneficial owner of a legal person, Section 21B(2) provides a step-by-step process of elimination which is to be followed by a firm, which is set out hereunder.

10.1 Overview of the Step-by-Step Process:

a. The **first step** is to identify the natural person who independently or together with another person has a Controlling Ownership Interest in a legal person.

- A controlling ownership interest relates to the ability of a natural person, by virtue of his or her ownership interest in a legal person, to control, take or influence decisions of the legal person, its resolutions and/or its business operations.

- Factors to be considered in determining whether a natural person has a controlling ownership interest in a legal person include:

  - the level of influence or control that the person exercises over the legal person;
  - the percentage of ownership interest that the person has in the legal person;
  - the level of influence, directly or indirectly, that the person has over the decisions of the legal person and/or its operations.

b. The **second step** is to identify the natural person who exercises Control by Other Means (if the determination of a natural person who holds a Controlling Ownership Interest proves to be indeterminate):

- If the beneficial owner of a legal person is not identified through step one, identify the natural person(s) exercising control by other means, such as through his or her ownership or control of other legal persons, partnerships, or trusts.

c. The **third step** is to identify the natural person(s) who exercises Control over the Management of the legal person (if the determination of a natural person(s) who holds a Controlling Ownership Interest or who exercises Control by Other Means proves to be indeterminate).

10.2 Step 1 – Controlling Ownership Interest:

a. **Definition**:

- "Controlling ownership interest" is the ability of a natural person, via ownership interest, to control/influence the legal person's resolutions, decisions or operations.

b. **Interpretative Factors**:

- influence over decisions and operations of a legal person;
- ownership interest percentage;
- level of influence or control exercised directly or indirectly.

RESOURCE:
The FIC has published Guidance Note 7A – Implementation of various aspects of the Financial Intelligence Centre Act, which is available at: https://www.fic.gov.za/wp-content/uploads/2025/02/2025.2-GN-implementation-of-fic-act.pdf

PCC 59 - Relating to Beneficial Ownership and the Application of Section 21B of the Financial Intelligence Centre Act, available at: https://www.fic.gov.za/wp-content/uploads/2024/08/PCC-59-Beneficial-ownership.pdf

c. **The Hybrid Approach**:

- A hybrid approach to determining controlling ownership interest combines a threshold approach with an overall assessment of ownership influence, as expanded on below.

d. **Factors to consider in a Hybrid Approach**:

- Indicator of Controlling Ownership Interest:

- The percentage of total ownership interest is an indicator of controlling ownership over a legal person.
- The FIC holds the view that the holding of five percent or more of ownership interest in a legal person is typically sufficient to exercise a controlling ownership interest.

- The FIC accordingly recommends that a firm identifies persons holding five percent or more of ownership interest in a legal person as beneficial owners for purposes of Section 21B(2).

    - The FIC determined the threshold of five percent with reference to the following factors:

        - Through Legislative Alignment with the Companies Act 2008 (Act 71 of 2008), regulation 32A, which requires affected companies to establish and maintain a register of persons who hold beneficial interest equal to or in excess of five percent of the total number of securities or class of securities.
        - Sector Risk Assessments highlighting the risk of legal person structures being abused by criminals who are beneficial owners.
        - Emerging Risks and Media Reports highlighting the abuse of the public procurement process using illegitimate companies with criminal beneficial owners.
        - The concealment of criminal beneficial owners using complex structures with multiple layers where a number of legal persons form a group with a natural person holding a small percentage of ownership interest across all entities in the structure, which aggregated provides a controlling ownership interest.

e. Considerations related to Ownership Structures:

- <u>Parallel Beneficial Ownership Structure:</u>

    - Parallel beneficial ownership structures refer to those instances where a natural person holds a small percentage ownership interest across multiple entities in a structure consisting of a group of legal persons.
    - Such ownership interest, when aggregated, may give rise to a controlling ownership interest.
    - A firm should therefore fully understand a legal person's ownership structure in order to be able to identify a parallel beneficial ownership structure.

f. **High-Risk Indicators for ML, TF, and PF**:

Where a firm assesses a legal person as high risk for ML, TF, or PF due to:

- The legal person being closely associated with a natural person who is an FPEP, a high-risk DPEP or a high-risk PIP;
- Significant adverse media coverage on the legal person and where there is further negative media coverage relating to natural persons who are holders of less than the five percent ownership interest;
- The legal person and/or associated natural persons being linked to reports or suspicions that the legal person or natural persons are linked to TF or PF;

a firm should consider also identifying such natural persons as beneficial owners.

g. **Types of Legal Persons and Forms of Ownership Interest**:

- Variation in Ownership Interest:

  Different legal persons have varied forms of ownership interest. For example, companies issue shares owned by shareholders and co-operatives issue membership shares owned by members. A firm should therefore have regard to a legal person's founding documents to identify the type of ownership interest issued.

- Influence and Decision-Making Power:

  Legal persons may have different sub-types of ownership interest which carry different weights concerning influence or decision-making power. A firm should therefore determine the different classes of beneficial ownership interest issued by a legal person.

- Beneficial Ownership Agreements:

  - There may further be instances where beneficial owners form coalitions or agreements in terms of which they take decisions regarding, or exercise influence over, a legal person in an aligned manner to exercise controlling influence together.
  - Such groups or coalitions of beneficial owners jointly hold the controlling ownership interest.
  - A firm should take reasonable steps to verify whether such coalitions or agreements exist when determining the ownership and control structure.

- Examples and Implementation:

  An example of an agreement referred to in the previous paragraph is a Shareholders' Agreement. Such an agreement may have as its purpose to protect the shareholders' investment, to establish a fair relationship between the shareholders or to govern how the company is run. Such agreements can involve all or only some of the shareholders (e.g., the holders of a particular class of share).

- Dispersed Shareholding:

  Where the shareholders are so dispersed that no natural person has a controlling ownership interest, a firm should proceed to the next level of the elimination process.

10.3 Step 2 – Exercising Control Through Other Means

a. **Doubts on Controlling Ownership Interest**:

If a firm doubts whether a natural person has a controlling ownership interest, or no natural person holds such an interest, a firm should establish whether, and if so, the identity of the natural person/s who exercise control of a legal person through other means. This would include through a natural person's ownership or control of other legal

persons, partnerships or trusts (see **General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 22 of 2022,** which amended Section 21B(2)(a)(ii) of FICA such that a firm has since the amendment been required to identify the natural person who exercises control via other legal persons, trusts, or partnerships).

b. **Examples through which Effective Control could be exercised through Other Means**:

- Power of Attorney;
- Nominee Shareholders;
- Debt Instruments or Financing Arrangements;
- Nominee Directors;
- Delegations of Authority or Delegated Authority in Law;
- Court Orders;
- Power to Appoint or Remove Majority of Board/Senior Managers;
- Power or Influence over decisions which impact profit;
- Formal or informal Contracts and Agreements;
- Nominee Arrangements;
- Board or Officer Appointments;
- Significant Influence on Corporate Decisions;
- Strategic Control;
- Formal and informal Agreements, provisions in Articles of Association/Partnership Agreements/Syndication Agreements and voting rights;
- Usufruct;
- Family Members or known Close Associates;
- External Parties; and
- Links with Family Members exercising Undue Influence.

c. **External Parties and Abnormal Transactions**:

Where a legal person transacts in a manner inconsistent with a firm's understanding of the legal person's business or which benefits an external party unduly, a firm should consider whether an external party is exercising control over the legal person and should consider applying CDD to identify any such party as a beneficial owner.

10.4 Step 3 – Exercises Control Over the Management:

a. Determining Control Over Management:

Where a firm is unable to identify the natural person/s who exercise control through ownership interest or other means, it is required to determine who the natural persons are who exercise control over the management of the legal person. This step should not supersede steps 1 and 2 of the process of elimination set out above. Furthermore, this step should be applied only in exceptional cases, once steps 1 and 2 have been exhausted and there are reasonable grounds as to why the beneficial owner could not be identified under steps 1 and 2.

b. Definition of Beneficial Owner – Effective Control:

A firm, when identifying the natural persons who exercise control over the management of a legal person, should read Section 21B(2)(a)(iii) with the definition of "beneficial owner", which refers to "effective control", the effect of which is that the reference to "management" in this Section does not include all levels of management within a legal person.

c. Legal Persons – Companies Listed on Exchanges:

A firm establishing a business relationship or conducting a single transaction with an exchange-listed company is required to comply with the requirements of Section 21B of FICA and thus to apply the elimination process when identifying beneficial owners. Exchanges have varying disclosure requirements relating to beneficial ownership. For example, public companies registered with CIPC are subjected to a beneficial ownership enquiry.

d. Foreign-Created Legal Persons:

A firm establishing a business relationship or conducting a single transaction with a foreign-created legal person is similarly required to comply with Section 21B of FICA and in this regard it may be necessary to engage the client or the entity responsible for the creation of the foreign legal person for beneficial ownership information.

e. Legal Persons – State-Owned Entities:

A firm, when dealing with a state-owned company, should identify the natural person who controls the legal person as the beneficial owner. A firm may follow either the second and/or third elimination stage. Certain state organs are incorporated as companies and must be identified as companies.

- There are, however, instances where government institutions are constituted as legal persons by statute. In these instances the governing statute should be reviewed to identify the natural persons who exercise effective control over the legal person, such as the board and accounting officer.

- A further government entity that is neither a company nor a legal person created by statute would include national, provincial, and local government departments. In these instances the beneficial owner would typically be the natural person exercising control over the management of the legal person.

f. Evidence of the Process of Elimination:

A firm is required to be in a position to provide evidence that it followed the three-step process of elimination provided for in Section 21B(2)(a). Failure to follow this process will result in a firm being seen as non-compliant with Section 21B(2)(a).

In the case of high-risk legal persons it may be prudent for a firm to identify all beneficial owner levels without elimination.

RESOURCE:

The FIC has published Guidance Note 7A – Implementation of various aspects of FICA, which is available at: https://www.fic.gov.za/wp-content/uploads/2025/02/2025.2-GN-implementation-of-fic-act.pdf

11. BENEFICIAL OWNERSHIP OF TRUSTS

11.1 Identification Requirements

A firm is required to identify all natural persons linked to a trust when establishing a business relationship with or conducting a single transaction with a trust. A firm is also required to identify all natural persons linked to a trust. Although decision-making power within a trust generally rests with a trustee, in practice the trustees, founders, donors, settlors, protectors and beneficiaries or categories of beneficiaries and other persons exercising effective control over a trust can all exercise influence over the decisions or operations of a trust.

Not only beneficiaries, but also trustees and founders can benefit from a trust. For example, a founder can use a trust as a vehicle to divest assets from the founder on paper while setting up the beneficiary structure within the trust in such a manner that the founder continues to benefit from the assets of the trust so divested. Criminals are aware that such a structure can be exploited for ML, TF and PF purposes.

It is also possible that external persons may be in a position to exercise undue influence over a trust or to extract a benefit from the trust without a legal connection to the trust. This may be possible due to a close association or affiliation with a trustee. For this reason it is important for a firm to monitor the transactions of a trust to ascertain whether such undue influence may be present and in so doing to mitigate this risk.

11.2 Mitigating ML, TF, and PF Risks:

In order to mitigate its ML, TF and PF risks, Section 21B(4) of FICA requires a firm to establish the identifying name and number of a trust, establish at which Master's office a trust is registered and to identify the founders, trustees and beneficiaries of a trust.

11.3 Trustee where Trustee is a Legal Person:

Where a trustee is a legal person with an appointed natural person as a representative trustee, a firm is required to identify the legal person trustee in terms of Section 21B(1). Furthermore, a firm is required to identify the beneficial owners of the legal person trustee through the process of elimination dealt with above. A firm would further be required to identify the authorised person who acts on behalf of the legal person trustee as the nominal trustee. The same would apply where a founder and/or a beneficiary is a legal person.

Similarly, where a founder of a trust is a person acting on behalf of a partnership or in pursuance of the provisions of a trust agreement, a firm is required to identify the partnership

or the trust in terms of Section 21B as well as the beneficial owners of the partnership or trust. It would also be required to identify the authorised person acting on behalf of the trust.

11.4 Beneficiaries of a Trust:

In respect of the beneficiaries of a trust, the firm must establish the identity of each beneficiary referred to by name in the trust deed or other instrument in terms of which the trust has been created.

If a beneficiary (who is referred to by name in the trust deed) is a legal person or a person acting on behalf of a partnership or in pursuance of the provisions of a trust deed, the firm must take reasonable steps to establish and verify the identities of the beneficial owners of those legal persons, partnerships or trusts.

If beneficiaries are not referred to by name in the trust deed or other instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined is to be established. The firm must take reasonable steps to verify these particulars.

11.5 Foreign Trusts:

Where a firm is dealing with a foreign trust and seeking to identify the beneficial owner, a firm is required to understand the ownership and control structure of the trust and to apply CDD measures in a similar manner as it would with domestic trusts. In complex matters, trust and company service providers and administrators may be involved and it may be necessary to engage with these trust and company service providers to determine the beneficial owner/s.

11.6 Trust-Like Structures:

Where a firm is dealing with a trust-like entity which functions in a similar manner to a trust, the same principles would apply as they would for a trust. An example of such a structure is a private foundation.

11.7 Foreign Trusts and Further Natural Persons:

It was mentioned above that during the CDD process relating to a trust, it was required of a firm to identify all natural persons linked to a trust, including the protector of a trust. A protector is usually of application when dealing with a foreign trust. A firm is required to identify the natural person in such an instance, as well as any other natural person linked to a foreign trust.

12. ESTABLISHING THE BENEFICIAL OWNERS OF PARTNERSHIPS

12.1 Identifying Partners:

A firm is required to identify and take reasonable steps to verify each partner within a partnership. This applies irrespective of the ownership percentage of each partner and includes every member of a partnership *en commandite*, an anonymous partnership or a similar partnership.

12.2 Partnerships, Partners who are Legal Persons, Partnerships or Trusts:

Where a partnership includes a partner who is a legal person or a natural person acting on behalf of a partnership or pursuant to a trust agreement, the beneficial owner of the legal person, partnership and trust is required to be identified. A firm is further required to establish the identity of the natural person who exercises executive control over the partnership.

12.3 Significant Control by One Partner:

There may be instances where a partner may exercise significant control over a partnership. Such instances may include the right to direct or veto management decisions such as investment decisions, the right to profit share or capital returns of the partnership's funds or assets, the right to amend the partnership's constitutional documents (e.g. the partnership agreement), the right to dissolve or convert the partnership or the right to partnership assets upon dissolution of the partnership.

RESOURCE:

The FIC has published Guidance Note 7A – Implementation of various aspects of FICA, which is available at: https://www.fic.gov.za/wp-content/uploads/2025/02/2025.2-GN-implementation-of-fic-act.pdf

13. ESTABLISHING THE BENEFICIAL OWNERS OF NPOs

A firm should follow a similar approach to NPOs as to that applied in relation to trusts. It should identify the founders of the NPO as well as the management of the NPO. Where beneficiaries are named, they should be identified. Where the beneficiaries are not named, the process via which beneficiaries are determined should be identified.

14. DEALING WITH A DOMESTIC POLITICALLY EXPOSED PERSON AND A PROMINENT INFLUENTIAL PERSON

If a firm determines that a prospective client with whom it engages to establish a business relationship, or the beneficial owner of that prospective client, is a domestic politically exposed person (DPEP) or a prominent influential person (PIP) as per Schedules 3A and 3C below and that, in accordance with its RMCP, the prospective business relationship entails a high risk, the firm is required to:

- obtain senior management approval for establishing the business relationship;
- 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.

PLEASE NOTE:

In terms of Section 21G, read with Section 42(2)(l), a firm is also required to determine whether an **existing client** is a DPEP or a PIP.

To identify whether a potential or existing client is a DPEP or a PIP, including whether a potential or existing client is an immediate family member or known close associate of a DPEP or PIP, a firm should, among others:

- obtain confirmation from a prospective or existing client as to whether he or she is a DPEP or PIP or an immediate family member or close associate of a DPEP or PIP;

- where applicable, conduct an online search to determine whether a prospective client is a DPEP or a PIP or an immediate family member or known close associate of a DPEP or PIP.

14.1 Determine risk profile:

A firm is required to determine whether a prospective or existing client that has been identified as a DPEP or PIP or an immediate family member or known close associate of a DPEP or PIP presents a high risk of ML, TF or PF to the firm.

14.2 Procedural steps:

If a prospective client or existing client identified as a DPEP or PIP or an immediate family member or known close associate of a DPEP or PIP presents a high risk, the required approval is to be obtained, reasonable measures should be applied to establish the source of wealth and source of funds and enhanced ongoing monitoring of the business relationship should be applied.

A firm, before obtaining the approval of senior management, should attempt to establish the source of wealth and source of funds of the prospective or existing client, which the client may confirm. A firm should further form an understanding of the prospective or existing client's wealth profile, e.g. shares, sale of assets, inheritance and sources of income, including employment income, directors' fees, offshore accounts, etc.

SCHEDULE 3A: DOMESTIC POLITICALLY EXPOSED PERSONS A domestic politically exposed person is an individual who: (a) holds, including in an acting position for a period exceeding six months, or has held a prominent public function in the Republic, including that of:	**YES**	**NO**
President or Deputy President of South Africa		
Government minister or deputy minister		
Premier of a province		
Member of the Executive Council of a province		
Executive mayor of a municipality		
Elected in terms of the Local Government: Municipal Structures Act, 1998		
Leader of a political party registered in terms of the Electoral Commission Act, 1996		
Member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003		
Head, accounting officer or chief financial officer of a national or provincial department or government component, as defined in Section 1 of the Public Service Act, 1994		
The municipal manager of a municipality or chief financial officer		
Chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of **a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 2003** (see list below)		
The chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in Section 1 of the Local Government: Municipal Systems Act, 2000		
A Constitutional Court judge or any other judge as defined in Section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001		
An ambassador or high commissioner or other senior representative of a foreign government based in the Republic		
An officer of the South African National Defence Force above the rank of major-general		
The position of head, or other executive directly accountable to that head, of an international organisation.		

SCHEDULE 3C: PROMINENT INFLUENCIAL PERSON	**YES**	**NO**
A prominent influential person is an individual who holds, or has held at any time in the preceding 12 months, the position of: a) chairperson of the board of directors; b) chairperson of the audit committee; c) executive officer; or d) chief financial officer, of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the *Gazette*.		

SCHEDULE 2 OR 3 TO THE PUBLIC FINANCE MANAGEMENT ACT

The Firm will consult the most recent version of the Public Finance Management Act to obtain the most recent version of the Schedules.

Schedule Two

This includes the following entities and any subsidiary or entity under the ownership control of the following entities:

Air Traffic and Navigation Services Company, Airports Company, Alexkor Limited, Armaments Corporation of South Africa, Broadband Infraco (Proprietary) Limited, Broadband Infraco Limited, CEF (Pty) Ltd, Denel, Development Bank of Southern Africa, Eskom, Independent Development Trust, Industrial Development Corporation of South Africa Limited, Land and Agricultural Bank of South Africa, SA Broadcasting Corporation Limited, South African Express (Proprietary) Limited, SA Forestry Company Limited, SA Nuclear Energy Corporation, SA Post Office Limited, South African Airways Limited, Telkom SA Limited, TransCaledon Tunnel Authority, Transnet Limited.

Schedule Three

This includes the following entities and any subsidiary or entity under the ownership control of the following entities:

Accounting Standards Board, Africa Institute of South Africa, Pretoria, African Renaissance and International Cooperation Fund, Afrikaanse Taalmuseum, Agricultural Research Council, AGRISETA, Artscape, Banking Sector Education and Training Authority, Boxing South Africa, Brand SA, BreedeGouritz Catchment Management Agency, Castle Control Board, Chemical Industries Education and Training Authority, Commission for Conciliation, Mediation & Arbitration, Community Schemes Ombud Service, Companies and Intellectual Property Commission, Companies Tribunal, Competition Commission, Construction Education and Training Authority, Construction Industry Development Board, Council for Built Environment (CBE), Council for Geoscience, Council for Medical Schemes, Council on Higher Education, Cross-Border Road Transport Agency, Culture, Arts, Tourism, Hospitality and Sports Education and Training Authority (CATHSSETA), Education, Training and Development Practices SETA (ETDP), Electricity Distribution Industry Holdings (Pty) Ltd, Electronic Communications Security (Pty) Ltd, Energy and Water Sector Education and Training Authority (EWSETA), Fibre Processing Manufacturing Sector Education and Training Authority (FPMSETA), Film and Publication Board, Financial and Accounting Services SETA (FASSET), Financial Intelligence Centre, Food and Beverages Manufacturing Industry (FOODBEV), Freedom Park Trust, Health and Welfare Sector Education and Training Authority, Housing Development Agency, Human Sciences Research Council, Independent Regulatory Board for Auditors, Information Systems, Electronics and Telecommunications Technologies Training Authority, Ingonyama Trust Board, Catchment Management Agency, Insurance Sector Education and Training Authority, International Trade Administration Commission, iSimangaliso Wetland Park, Iziko Museums of South Africa, KwaZulu Natal Museum, Legal Aid South Africa, Local Government Education and Training Authority (LGSETA), Manufacturing, Engineering and Related Services Education and Training Authority, Marine Living Resources Fund, Market Theatre Foundation, Media Development and Diversity Agency, Media, Information and Communication Technologies Sector Education and Training Authority (MICTS), Mine Health & Safety Council, Mining Qualifications Authority, Municipal Infrastructure Investment Unit, National Agricultural Marketing Council, National Arts Council, National Consumer Commission, National Consumer Tribunal, National Credit Regulator, National Development Agency, National Economic, Development and Labour Council, National Electronic Media Institute of SA, National Empowerment Fund, National Energy Regulator of South Africa, National Film and Video Foundation, National Gambling Board of SA, National Health

Laboratory Service, National Heritage Council (NHC), National Home Builders Registration Council (NHBRC), National Housing Finance Corporation, National Library, Pretoria/Cape Town, National Lotteries Commission, National Metrology Institute of South Africa, National Museum, Bloemfontein, National Nuclear Regulator, National Regulator for Compulsory Specifications, National Research Foundation, National Student Financial Aid Scheme, National Urban Reconstruction and Housing Agency, National Youth Development Agency, Nelson Mandela Museum, Umtata, Office of Health Standards Compliance, Office of the Ombudsman for Financial Services Providers, Office of the Pension Funds Adjudicator, Performing Arts Council of the Free State, Perishable Products Export Control Board, Private Security Industry Regulatory Authority, Productivity SA, Public Service Sector Education and Training Authority (PSETA), Quality Council for Trades and Occupations (QCTO), Railway Safety Regulator, Road Accident Fund, Road Traffic Infringement Agency (RTIA), Road Traffic Management Corporation, Robben Island Museum, Cape Town, Rural Housing Loan Fund, Safety and Security Sector Education and Training Authority (SASSETA), SA Civil Aviation Authority, SA Council for Educators, South African Diamond and Precious Metals Regulator, SA Heritage Resources Agency, SA Library for the Blind, SA Local Government Association, SA Maritime Safety Authority, SA Medical Research Council, SA National Accreditation System, South African Health Products Regulatory Authority (SAHPRA), South African National Biodiversity Institute (SANBI), South African National Energy Development, Institute (SANEDI), South African National Parks, SA National Roads Agency, South African National Space Agency, SA Qualifications Authority, SA Revenue Service, South African Social Security Agency, SA Tourism Board, South African Weather Service, Servcon, Small Enterprise Development Agency (SEDA), Special Investigation Unit, State Information Technology Agency, State Theatre, Pretoria, The Cooperative Banks Development Agency, The National English Literary Museum, Grahamstown, The National Radioactive Waste Disposal Institute (NRWDI), The National Skills Fund (NSF), The Playhouse Company, Durban, The Social Housing Regulatory Authority (SHRA), Thubelisha Homes, Tourism and Hospitality Education and Training Authority, Transport Education and Training Authority, uMalusi Council for Quality Assurance in General and Further Education and Training, Unemployment Insurance Fund, Universal Service and Access Agency of South Africa, Universal Service and Access Fund, Urban Transport Fund, War Museum of the Boer Republics, Bloemfontein, Water Research Commission, Wholesale and Retail Sector Education and Training Authority, William Humphreys Art Gallery.

Part B: National Government Business Enterprises

Amatola Water Board, Aventura, Bloem Water, Council for Scientific and Industrial Research (CSIR), Export Credit Insurance Corporation of South Africa Limited, Inala Farms (Pty) Ltd, Lepelle Northern Water, Magalies Water, Mhlathuze Water, Mintek, Ncera Farms (Pty) Ltd, Onderstepoort Biological Products, Overberg Water, Passenger Rail Agency of South Africa, Public Investment Corporation Limited, Rand Water, SA Bureau of Standards (SABS), Sasria Limited, Sedibeng Water, Sentech, State Diamond Trader, Umgeni Water.

Part C: Provincial Public Entities – as listed under the Schedule.
Part D: Provincial Government Business Enterprises – as listed under the Schedule.

15. DEALING WITH A FOREIGN POLITICALLY EXPOSED PERSON

A firm is required to follow a similar process to that of high-risk DPEPs or PIPs or immediate family members or known close associates of DPEPs or PIPs, as set out above, in relation to a foreign politically exposed person (FPEP), as listed under Schedule 3B, of FICA or to an immediate family member or known close associate of an FPEP, save that irrespective of the risk rating of the FPEP or immediate family member or known close associate of an FPEP, the steps referred to are required to be carried out. An FPEP is an individual who holds, or has held, in any foreign country a prominent public function including that of a:

a. Head of State or head of a country or government;
b. member of a foreign royal family;
c. government minister or equivalent senior politician or leader of a political party;
d. senior judicial official;
e. senior executive of a state-owned corporation; or
f. high-ranking member of the military.

16. NOT ESTABLISHING AND TERMINATING A BUSINESS RELATIONSHIP

A firm is not permitted to establish a business relationship or to conclude a single transaction with a client if it is unable to:

a. establish and verify the identity of a client or other relevant person as required under FICA;

b. obtain information to reasonably enable a law firm to determine whether future transactions that will be performed in the course of the business relationship concerned are consistent with the firm's knowledge of that prospective client;

c. conduct ongoing due diligence as required under FICA.

If a firm is unable to establish the above with reference to an existing client relationship:

- the relationship with the client is required to be terminated; and
- consideration should be given as to whether a report should be submitted pursuant to FICA.

17. ONGOING DUE DILIGENCE [AND MONITORING OF ML/TF/PF RISKS]

A firm, in the context of an extended client relationship, is likely to be exposed to changes in the client's risk profile. A firm is therefore required to conduct regular ongoing due diligence to ensure, *inter alia*, that the transactions being conducted during the business relationship are consistent with the firm's knowledge of the client and the client's business and risk profile. The frequency of ongoing due diligence will be determined by the risk-rating of the client.

17.1 The degree of ongoing monitoring

The degree of ongoing monitoring is dependent on several factors, including:

a. the size of a firm and its available resources;

b. the risk profile of the client, as assessed at the inception of the client relationship;

c. the nature of changes that have occurred since inception of the client relationship;

d. changes in sources of funds which the client may have accessed; and

e. instructions to execute further risk-related services or transactions.

A firm is also required to examine:

- complex or unusually large transactions; and
- unusual patterns of transactions which have no apparent business or lawful purpose,
- and to retain written findings in respect thereof.

17.2 Factors to be considered:

An examination of such transactions may take into account the following factors:

a. the nature of the legal services required and underlying purpose;

b. the legislation, regulatory requirements and industry standards (or lack thereof) applicable to the transactions;

c. the unusual and disproportionate amounts involved and disparate exchange of value;

d. the sourcing of substantial funds from high-risk countries without any apparent linkage;

e. the rendering of services that are mismatched within the context;

f. the use of multiple bank accounts without any apparent reason;

g. deposits of large sums of money without genuine business activities or acumen;

h. unusual payment instructions taking into consideration industry practices;

i. increase of assets or income in either local or foreign countries without plausible economic justification;

j. substantially large financial transactions for recently incorporated entities without any apparent economic reason; and

k. substantially large financial transactions that are unsuitable for the prospective client's business profile or commercial status.

18. PERSONS & ENTITIES IDENTIFIED BY THE UN's SECURITY COUNCIL

A firm is required to ensure that no legal service or other activity relating to property, financial or other services or economic support, as the case may be, falling within the ambit of Section 26B(1) of FICA is rendered or made available to persons or entities that have been identified by resolution of the Security Council of the United Nations, and in terms of which and in respect of whom financial sanctions have been imposed.

A firm is required to introduce suitable controls to ensure that no legal practitioner or employee at the firm directly or indirectly deals with, enters into or facilitates any transaction or performs any other act in connection with property which he or she knows or ought reasonably to have known or suspected to have been acquired, collected, used, possessed, owned or provided for the benefit of, or on behalf of, or at the direction of, or under the control of a person or an entity identified pursuant to a resolution of the UN's Security Council referred to in Section 26A(1) of FICA.

A firm is required to further introduce suitable controls to ensure that no legal practitioner or employee at the firm assists or becomes involved in a service which will have the effect of aiding in the retaining, controlling, converting, concealing, transferring, removing or disguising the nature, source, location, disposition or movement of property, for the benefit of persons or entities that have been identified pursuant to a resolution by the Security Council of the United Nations referred to in Section 26A(1) of FICA.

A firm should regularly review the resolutions adopted by the Security Council of the United Nations under Chapter VII of its Charter referred to in Section 26A(1) of FICA, as circulated by the FIC from time to time.

The TFS List can be accessed on the FIC's website at:
https://tfs.fic.gov.za/Pages/TFSListDownload

Importantly, the FIC's PCC 44A provides as follows:

a. This prohibition under Section 26B of the FIC Act is applicable, but not limited to, all instances where the designated person or entity is:
   - the client;
   - the person acting on behalf of the client;
   - the client acting on behalf of another person;
   - a beneficial owner of the client; or
   - a party to a client's transaction, including a party who benefits in any way from a client's transaction.

b. The firm is required to scrutinise its information concerning clients with whom the firm has a business relationship, including the persons listed above, against the TFS List, to determine if any persons are designated persons or entities or linked to designated persons or entities. Screening is required for both domestic and international transactions. The firm should be able to demonstrate that it has complied with this requirement.

c. The FIC requires that firms scrutinise information concerning clients with whom the firm seeks to conclude a single transaction against the TFS Lists as published on the Centre's website.

d. The results from the screening will inform the risk rating.

e. A firm is not permitted, directly or indirectly, to transact with or to process a transaction for a designated person or entity.

f. Adequate scrutinising must take place at the appropriate frequency and intensity.

g. Failure to identify that a person is listed as or linked to a designated person or entity, is regarded as non-compliance.

h. The information that should be used for scrutinising includes:

- the person's name;
- identification number;
- place of birth;
- address;
- date of birth;
- nationality;
- entity's name and other information;

i. The screening should happen:

- at client onboarding;
- when conducting transactions;
- when the TFS List is updated.

Importantly, all existing information concerning clients must be scrutinised against the TFS List as and when the TFS List is updated.

RESOURCES: The following resource should be consulted:

- The FIC's Public Compliance Communication 44A – Implementation of Targeted Financial Sanctions in South Africa.

19. TRAINING

A firm should adopt relevant policies to guide the implementation of its RMCP and ensure that training is offered to its attorneys and staff members. Section 43 of FICA requires the firm to provide ongoing training to its employees to enable them to comply with the provisions of FICA and the RMCP which are applicable to them.

20. REPORTING REQUIREMENTS

A firm is required to comply with the reporting requirements provided for in FICA. These are set out under Sections 28, 28A, 29 and 31.

A firm should ensure that:

a. all regulatory reports are submitted via the FIC's goAML portal;
b. users log in with their own user credentials to submit reports;
c. the correct report type is selected;
d. reports are submitted under the correct branch and the correct Schedule item number; and
e. reports are meticulously completed and reviewed before being submitted.

20.1 Section 28: Cash Threshold Reports (CTR)

a. This reporting requirement is triggered by cash transactions above the threshold of **R49 999.99**.

b. The cash threshold is applicable to cash transactions, i.e.:
   - Coins and paper money; and
   - Travellers' cheques;

   and is not applicable to transactions made via EFT.

c. A firm is required, **within three business days** of becoming aware of a cash transaction that exceeds the prescribed limit, to comply with this reporting requirement.

d. The requirement is applicable where the cash amount is:
   - paid by a firm to a client, or to a person acting on behalf of a client, or to a person on whose behalf a client is acting; and
   - received by a firm from a client, or from a person acting on behalf of a client, or from a person on whose behalf a client is acting.

e. The Firm should refer to the exchange rate at the time of the transaction if foreign currency forms part of the transaction.

f. If the cash received from a client and the cash paid out to a client by a firm both exceed the threshold amount, two cash threshold reports are required to be submitted to the FIC.

A firm should have regard to the requirements set out in Regulations 22C and 24 of FICA in regard to the information to be included in a CTR and the reporting period.

20.2 Section 28A: Terrorist Property Report (TPR)

A firm is required, in terms of Section 28A(1) read with Section 26A(1) and Section 28A(3), to scrutinise its client information against the Targeted Financial Sanctions list (TFS List).

A firm is not permitted to establish a business relationship with and/or to conduct a single transaction on behalf of a person appearing on the TFS List.

A firm is furthermore required to file a TPR with the FIC if the firm has in its possession or under its control property owned or controlled by, or on behalf of, or at the direction of:

a. any entity which has committed or attempted to commit or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA); and
b. a person or entity identified pursuant to a resolution of the United Nations Security Council contemplated in Section 26A(1) of FICA (i.e. a person appearing on the TFS List).

A firm is required, **within five days** of becoming aware that it has property associated with terrorist and related activities in its possession or under its control, to file a TPR with the FIC. A firm should have regard to the requirements set out in Regulations 22A and 24 of FICA in regard to the information to be included in a TPR and the reporting period.

20.3 Section 29: Suspicious or Unusual Transaction Report (STR), Suspicious or Unusual Activity Report (SAR), Terrorist Financing Transaction Report (TFTR) and Terrorist Financing Activity Report (TFAR)

A firm is required to file a report in terms of Section 29 when it knows or ought reasonably to have known or suspected that:

a. the firm has received or is about to receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
b. a transaction or series of transactions to which the firm is a party:
    - facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist related activities;
    - has no apparent business or lawful purpose;
    - is conducted for the purpose of avoiding giving rise to a reporting duty under FICA;
    - may be relevant to the investigation of tax evasion or attempted tax evasion;
    - relates to an offence relating to the financing of terrorist and related activities; or
    - relates to the contravention of a prohibition under Section 26B of FICA;
c. the firm has been used or is about to be used for ML or TF purposes.

Where a firm knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or those transactions had been concluded, have had any of the above consequences, the firm is required to file a report in terms of Section 29.

In terms of Section 21E, a firm should consider submitting a Section 29 report to the FIC should it be unable to:

a. establish and verify the identity of a client and other relevant persons in terms of Section 21 or 21B;
b. obtain information concerning the business relationship and source of funds contemplated in Section 21A;
c. conduct ongoing due diligence as contemplated in Section 21C.

Note that there is no monetary threshold applicable to the reporting of suspicious or unusual transactions.

20.4 Suspicious and unusual transaction report

A firm is required to submit an STR where the suspicion is in respect of a complete transaction or series of transactions relating to the suspicion or knowledge of the proceeds of unlawful activity or money laundering and regarding a transaction or series of transactions relating to a contravention of prohibitions under Section 26B of FICA.

20.5 Suspicious and unusual activity report

A Firm is required to submit a SAR where a suspicion relates to the proceeds of unlawful activity, or money laundering activity or a contravention of prohibitions under Section 26B of FICA:

a. where the report relates to an activity which does not involve a transaction between two or more parties;

b. in respect of a transaction or a series of transactions about which enquiries are made but which has not been concluded; or

c. in respect of a transaction which has been interrupted, aborted, abandoned or is incomplete and ultimately not concluded.

20.6 Terrorist financing activity report

A firm is required to submit a TFAR where a suspicion relating to the financing of terrorist and related activities:

a. relates to an activity which does not involve a transaction between two or more parties; or

b. is in respect of a transaction or a series of transactions about which enquiries were made but which had not been concluded.

20.7 Terrorist financing transaction report

A firm is required to submit a TFTR where the suspicion is in respect of a transaction, or a series of transactions, relating to terrorist financing and related activities.

20.8 Relationship with a client

A firm is permitted, in terms Section 33 of FICA, to continue with and carry out a transaction in respect of which a report is required to be made in terms of Sections 28 and 29, unless the FIC directs the firm not to proceed with the transaction.

The FIC may, in terms Section 34 of FICA, direct a firm in writing not to proceed with a transaction for a period not longer than 10 days.

20.9 Definition: Knowledge of a Fact

To assist with the interpretation of Section 29, knowledge of a fact is defined in FICA as follows:

In terms of Section 1(2) of FICA, a person has knowledge of a fact if:

a. the person has actual knowledge of that fact; or

b. the court is satisfied that the person believes that there is a reasonable possibility of the existence of that fact; and the person fails to obtain information to confirm or refute the existence of that fact.

20.10 Definition: Suspicion

The Supreme Court of Appeal has, in the matter of *Powell NO and Others v Van der Merwe and Others (503/2002) [2004] ZASCA 25*, confirmed its endorsement of the following definition:

> *"'Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking; 'I suspect but I cannot prove'. Suspicion arises at or near the starting point of an investigation of which the obtaining of prima facie proof is the end."*

IMPORTANT – TIPPING OFF

No person, and concomitantly a firm, involved in the making of a report in terms of Section 29 may disclose that fact or the contents of such a report to any other person, including the person in respect of whom the report is or must be made otherwise than as required by law.

A Section 29 report should be submitted to the FIC as soon as possible after a firm becomes aware of a fact which gave rise to the knowledge or suspicion, but not later than **15 days**, excluding Saturdays, Sundays and Public Holidays, of becoming so aware.

PLEASE NOTE:

1. Discontinuation of CDD Process: If a firm suspects that a transaction or activity is suspicious or unusual as contemplated in Section 29, and reasonably believes that performing the CDD requirements in terms of this Section will disclose to the client that a Section 29 report will be made, it may discontinue the CDD process and consider making a Section 29 report.

2. Repeat of CDD Process: A firm is required to repeat the steps contemplated in Sections 21 and 21B (to the extent that this is necessary to confirm the information previously obtained) **if** it:

   a. doubts the veracity or adequacy of previously obtained information; or

   b. makes a suspicious or unusual transaction report in terms of Section 29.

20.11 Section 31: Cross-border money movement (IFTR)

Certain categories of AIs who, through electronic transfer, send money in excess of the prescribed amount (presently R19 999) out of South Africa or who receive money in excess of the prescribed amount from outside South Africa on behalf, or on the instruction, of another person, such AIs are required, within the prescribed period after the money was transferred, to report the transfer, together with the prescribed particulars concerning the transfer, to the FIC.

This requirement is only applicable, however, to AIs that are authorised in terms of the regulations under the Currency and Exchanges Act, 1933 (Act 9 of 1933) (Exchange Control Regulations) to conduct authorised transactions under these regulations.

21. RECORD-KEEPING

A firm is required to retain a record of the information required and obtained under Sections 21 to 21H of FICA, which includes information relating to:

a. the verification of a client's identity;

b. with reference to a business relationship, the nature and intended purpose of the business relationship and the source of the funds which the prospective client is expected to use in concluding transactions in the course of the business relationship.

c. every transaction, whether the transaction is a single transaction or concluded in the course of a business relationship which a law firm has with a client, that is reasonably necessary to enable that transaction to be readily reconstructed, which information must, among others, include the following information:

- the amount and currency involved;
- the parties to and date on which the transaction was concluded;
- the nature of the transaction; and
- business correspondence.

A firm is required, among others, to keep the records which relate to:

- the establishment of a business relationship for at least five years from the date on which the business relationship terminated; and
- a transaction or activity which gave rise to a report contemplated in Section 29, for at least five years from the date on which the report was submitted to the FIC.

22. CONFIDENTIALTY AND LEGAL PROFESSIONAL PRIVILEGE

It should also be noted that subject to Legal Professional Privilege, Section 37(1) of FICA provides that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by a firm with a provision of Part 3 (Reporting Duties and Access to Information), Part 4 (Measures to Promote Compliance by Accountable Institutions) and Chapter 4 (Compliance and Enforcement) of FICA.

What is Legal Professional Privilege?

The Constitutional Court[3] has confirmed the following features with reference to Legal Professional Privilege:

1. The right to Legal Professional Privilege is a general rule of our common law which states that communications between a legal advisor and his or her client are protected from disclosure, provided that certain requirements are met.

2. It is now generally accepted that the rationale of this right is that communications should be protected in order to facilitate the proper functioning of an adversarial system of justice.

3. Legal Professional Privilege encourages full and frank disclosure between advisors and clients. This promotes fairness in litigation.

4. The common-law right to Legal Professional Privilege must be claimed by the right-holder or by the right-holder's legal representative.

The Western Cape High Court[4] has listed the following requirements in relation to Legal Professional Privilege:

1. The legal advisor must have been acting in a professional capacity at the time;

2. The advisor must have been consulted in confidence;

3. The communication must have been made for the purpose of obtaining legal advice;

4. The advice must not facilitate the commission of a crime or fraud; and

5. The privilege must be claimed.

The Court reiterated that the character of the rule is accepted to be substantive rather than procedural and held that: "A party that asserts Legal Professional Privilege should generally be able to provide a rational justification for its claim without needing to disclose the content or substance of the matter in respect of which the privilege is claimed."

23. SCREENING AND SCRUTINISING OF CURRENT AND PROSPECTIVE EMPLOYEES

The firm is required to provide for and record the process and manner in which it screens prospective and current employees for competence and integrity and scrutinises said employees against the TFS List. The firm is required to keep record of the outcome of the screening and scrutinising, which must be made available to the FIC upon request.

RESOURCES: The FIC has published:
Directive 8 of 2023

[3] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma v National Director of Public Prosecutions and Others* 2009 (1) SA 1 (CC)
[4] *A Company and Others v Commissioner, South African Revenue Service* 2014 (4) SA 549 (WCC)

Public Compliance Communication 55 on Directive 8, which provides guidance to accountable institutions on the application of Directive 8.

24. KEY DEFINITIONS

The following meaning has been ascribed to the following terms:

24.1 **"Unlawful activity"** – "conduct which constitutes a crime or which contravenes any law, whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere."

24.2 "**Law firm/Firm**" means attorneys practising for their own account and as part of a commercial juristic entity contemplated in Sections 34(5) and 34(7) of the Legal Practice Act 28 of 2014.

24.3 "**Money laundering**" or "**money laundering activity**" per Section 1 of FICA means an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of Section 64 of FICA or Sections 4, 5 or 6 of the Prevention of Organised Crime Act.

Sections 4, 5 and 6 of POCA are, respectively entitled: *Money laundering* (s 4); *Assisting another to benefit from proceeds of unlawful activities* (s 5); and *Acquisition, possession or use of proceeds of unlawful activities* (s 6).

Section 4 of POCA provides that: "*Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and:*

(a) enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or

(b) performs any other act in connection with such property, whether it is performed independently or in concert with any other person, which has or is likely to have the effect –

(i) of concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof; or

(ii) of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere:

(aa) to avoid prosecution; or

(bb) to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence, shall be guilty of an offence."

Section 5 of POCA provides that: "*Any person who knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities, and who enters into any agreement with anyone or engages in any arrangement or transaction whereby:*

(a) the retention or the control by or on behalf of the said other person of the proceeds of unlawful activities is facilitated; or
(b) the said proceeds of unlawful activities are used to make funds available to the said other person or to acquire property on his or her behalf or to benefit him or her in any other way, shall be guilty of an offence."

Section 6 of POCA provides that: "*Any person who:*
(a) acquires;
(b) uses; or
(c) has possession of,
property and who knows or ought reasonably to have known that it is or forms part of the proceeds of unlawful activities of another person, shall be guilty of an offence."

24.4 Section 1 of POCDATARA defines "**terrorist activity**", with reference to Sections 1, 2, 3 and 17(2) of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA), means any act –

(a) committed in or outside the Republic, which:

i. involves the systematic, repeated or arbitrary use of violence by any means or method;

ii. involves the systematic, repeated or arbitrary release into the environment or any part of it or distributing or exposing the public or any part of it to:

(aa) any dangerous, hazardous, radioactive or harmful substance or organism;

(bb) any toxic chemical;

(cc) any microbial or other biological agent or toxin; or

(dd) any weapon of mass destruction in terms Section 1 of the Non-Proliferation of Weapons of Mass Destruction Act, including those with dual-purpose capabilities as defined in Section 1 of the Non-Proliferation of Weapons of Mass Destruction Act, or any substance, mixture of substances, product or material contemplated in Section 2(1) of the Hazardous Substances Act;

iii. endangers the life of, or violates the physical integrity or physical freedom of, or causes serious bodily injury to or the death of, any person, or any number of persons;

(iiiA) is calculated to overthrow the government of the Republic or any other government;

iv. causes serious risk to the health or safety of the public or any segment of the public;

v. causes the destruction of or substantial damage to any property, natural resource, or the environmental or cultural heritage, whether public or private;

(vA) causes the destruction of or substantial damage or interference to an information infrastructure or any part thereof;

vi. is designed or calculated to cause serious interference with or serious disruption of an essential service, facility or system, or the delivery of any such service, facility or system, whether public or private, including, but not limited to:

(aa) a system used for, or by, an electronic system, including an information system;

(bb) a telecommunication service or system;

(cc) a banking or financial service or financial system;

(dd) a system used for the delivery of essential government services;

(ee) a system used for, or by, an essential public utility or transport provider;

(ff) an essential or critical infrastructure, information infrastructure, or a critical infrastructure complex; or

(gg) any essential service designated as such in terms of the Labour Relations Act, 1995 (Act No. 66 of 1995), or essential emergency services, such as police, medical or civil defence services;

vii. causes any major economic loss or extensive destabilisation of an economic system or substantial devastation of the national economy of a country;

viii. creates a serious public emergency situation or a general insurrection in the Republic; or

ix. is the offence of:

(aa) unlawful access in terms of Section 2 of the Cybercrimes Act;

(bb) unlawful interception of data in terms of Section 3 of the Cybercrimes Act;

(cc) unlawful interference with data or a computer program in terms of Section 5 of the Cybercrimes Act;

(dd) unlawful interference with a computer data storage medium or a computer system in terms of Section 6 of the Cybercrimes Act;

(ee) unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data or device in terms of Section 7 of the Cybercrimes Act;

(ff) unlawful use or possession of a software or hardware tool for purposes of committing the offences listed in items (aa) to (ee); or

(gg) cyber extortion in terms of Section 10 of the Cybercrimes Act, which is committed with the intention to facilitate or to commit an act referred to in subparagraphs (i) to (viii) of this paragraph, whether the harm contemplated in subparagraphs(i) to (vii) is or may be suffered in or outside the Republic, and whether the activity referred to in subparagraphs (ii) to (ix) was committed by way of any means or method; and

(b) which is intended, or by its nature and context, can reasonably be regarded as being intended, in whole or in part, directly or indirectly, to –

(i) threaten the unity and territorial integrity of the Republic;

(ii) intimidate, or to induce or cause feelings of insecurity within the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population;

(iii) unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organisation or body or intergovernmental organisation or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles; or

(iv) further the objectives of an entity engaged in terrorist activity,

whether the public or the person, government, body, or organisation or institution referred to in subparagraphs (ii) or (iii), as the case may be, is inside or outside the Republic.

24.5 **Proliferation financing activity,** as defined in Section 1 of FICA, means an activity which has or is likely to have the effect of providing property, financial or other service or economic support to a non-State actor, that may be used to finance the:

- manufacture,
- acquisition,
- possessing,
- development,
- transport,
- transfer, or
- use of

nuclear, chemical or biological weapons of mass destruction and their means of delivery and includes any activity which constitutes an offence in terms of Section 49A of FICA.

25. REFERENCE LIST

	TITLE
1.	**Reference Guide for All Accountable Institutions** to assist all new, and existing accountable institutions.
2.	**Guidance Note 4B** on Reporting of suspicious and unusual transactions and activities to the Financial Intelligence Centre in terms of Section 29 of the Financial Intelligence Centre Act
3.	**Guidance Note 5C** on cash threshold reporting to the Financial Intelligence Centre in terms of Section 28 of the Financial Intelligence Centre Act
4.	**Guidance Note 6A** on Terrorist financing and terrorist property reporting obligations in terms of Section 28A of the Financial Intelligence Centre Act.
5.	**Guidance Note 7A** on the implementation of various aspects of the Financial Intelligence Centre Act
6.	**PCC 44A** - Implementation of targeted financial sanctions.
7.	**PCC 53** - on the Risk Management and Compliance Programme in terms of Section 42 of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) for DNFBPs.
8.	**PCC 55** – on Directive 8 screening of employees for competence and integrity and scrutinising of employee information against targeted financial sanctions lists as a money laundering, terrorist financing and proliferation financing control measure.
9.	**PCC 59** - Relating to beneficial ownership and the application of Section 21B of the Financial Intelligence Centre Act
10.	User Guide: STR
11.	User Guide: Remediating Reports – Targeted Financial Sanctions Manual
12.	User Guide: Remediating Reports – goAML Registration Guide
13.	The South African National Terrorism Financing Risk Assessments of 31 March 2022 and 24 June 2024. The risk assessments focus on, inter alia, the threats, vulnerabilities and possible impact of terror financing on South Africa's safety and stability.
14.	The Assessments of the Inherent Money Laundering and Terrorist Financing Risks: Legal Practitioners of March 2022 and March 2024. The risk assessments focus on the legal practitioners' sector.

Please note that the FIC specifically states that:

Guidance provided 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 FICA and the MLTFC Regulations.