consult.
by momentum

Momentum Consult (Pty) Ltd ("Consult")

Risk Management and Compliance Programme (RMCP)

1. Version control

Policy level:	Board approved
Applicable principal risk:	Regulatory
Principal risk owner:	Chief Executive Officer (CEO): Consult
Effective date:	2 April 2019
Last review date:	December 2022 - June 2023
Next review date:	June 2024 – June 2027
Policy co-ordinator:	Consult Compliance
Approved by:	Consult Board of Directors
Adopted by:	Consult Executive Committee
Board Approval date:	November 2019

Document Status

Version	2
Ownership	MC Compliance Function
Document Status	Board Approval of amendments pending
Document Location	InConsultation
Author	Jackie Drotsky: Regulatory Compliance Manager

Version History and Distribution

Date	Version	Summary Of Changes	Distribution	Board approved?
November 2019	1	Implementation of RMCP	MC All	Yes
November 2021	1.1	Name change update	MC All	No. No material changes
December 2022 – June 2023	2	Annual Review 1. The inclusion of immediate family members or known close associates of a DPIP or FPPO as a high-risk person; 2. Update of the compliance checklist in terms of verification documents required for CDD purposes;		Reviewed by Group Compliance and CAF; to be tabled at Board

Date	Version	Summary Of Changes	Distribution	Board approved?
		3. Inclusion of the requirement for Financial Advisers to screen clients against sanction lists on National Treasury's website; 4. Inclusion of PCC 115 – Proliferation financing; 5. Inclusion of PCC 22A on information processing in terms of the Financial Intelligence Centre Act 38 of 2001, in relation to data protection; 6. Inclusion of Directive 6/2022 and draft public compliance communication 116: on screening of employees for competence and integrity as well as scrutinising employee information against the targeted financial sanctions lists by Consult; 7. Inclusion of Guidance note 102A: on processing of electronic funds transfers; and 8. Inclusion of Directive ID1 of 2022: in terms of section 43A(2) of the FIC Act (beneficiaries of life insurance policies); 9. Inclusion of FIC Directive 8, which requires the screening of employees for competence and integrity and scrutinising of employee information against applicable targeted financial sanctions lists as a money laundering, terrorist financing and proliferation financing control measure.		

2. Risk Management and Compliance Programme (RMCP) – Document Information

The RMCP is a documented record of Consult's control measures and efforts to comply with its obligations under FICA on a "risk sensitive" basis.

Below follows the minimum requirements of a RMCP and this document is therefore structured to address these minimum requirements: -

a) Document, maintain and implement a RMCP;
b) Incorporate all the elements in FICA that are linked to Client Due Diligent Measures (CDD);
c) Describe the application and implementation of measures of Consult's Risk Based Approach that will as a minimum include: -
   - The end-to-end CDD process, i.e., from establishing a business relationship, on-boarding a client, on-boarding of financial advisers, ongoing monitoring of client behaviour, to termination of the relationship with recordkeeping of all relevant client detail and transaction information;
   - Ongoing CDD processes in handling High Risk clients or status changes to a client's risk profile from Low to High Risk;
   - Measures to deal with doubt about the veracity of previously obtained CDD information;
   - Measures to deal with suspicion of ML or TF activities formed post client on-boarding; and
   - Measures to prevent the entering into or maintaining a business relationship if Consult cannot perform CDD, and the manner in which Consult will terminate an existing business relationship when unable to complete CDD requirements, etc.
d) Describe implemented governance processes, for example, related to executing reporting obligations, training programs, monitoring programs etc.

3. Purpose of the Risk Management and Compliance Programme

The Financial Intelligence Centre Amendment Act ("FICA: Act 1 of 2017") is formal legislation intended to combat money laundering activities by establishing a Financial Intelligence Centre ("FIC") and imposing certain duties on institutions and other persons, where such persons' or institutions' services or products offered to clients may be used for money laundering purposes. These persons/institutions are in most instances clearly defined in the Act as "Accountable Institutions (AI)" but there are also some general duties imposed on other persons.

Apart from criminalising the act of money laundering, South African law also imposes a number of control measures that must be adhered to which are aimed to facilitate the prevention, detection and investigation of money laundering or terrorist financing activities.

These control measures introduced by FICA include requirements for institutions to establish and verify the identities of their clients, to keep certain records, to report certain information and to implement measures that will assist them in complying with the Act. To achieve this FICA further imposes on Accountable Institutions the requirement to implement a formal Anti-money laundering (AML), Counter-Terrorist Financing (CTF) and Proliferation Financing (PF) Risk Management and Compliance programme (RMCP).

This document is therefore prepared in compliance with Section 42 of FICA to advise employees on the specific duties of all employees, which flow from the requirements of the Act.

It is thus of paramount importance that all employees of Consult understand and adhere to the contents of this document to avoid financial loss and reputational damage to Consult and to avoid being held personally liable and accountable under the provisions of the Financial Intelligence Act.

4. Introduction

Combating Money Laundering, Terrorist Financing and Proliferation Financing is the responsibility of everyone

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for the combating of money laundering, terrorist financing, and other related threats to the integrity of the international financial system.

South Africa is a member of the Financial Action Task Force (FATF) and as such have subscribed to the FATF Recommendations. The FATF Recommendations have been endorsed by over 200 countries and are universally recognised as the international standard for anti-money laundering, countering the financing of terrorism and proliferation financing.

The South African government has demonstrated its commitment to combating money laundering, terrorist financing and proliferation financing by implementing appropriate measures through the promulgation of FICA in order to introduce transparency in the South African financial system (based on robust customer due diligence measures). This will ensure that adequate information is captured in the records of financial and other institutions and to make the sharing of information that may support further investigation of money laundering, terrorist financing and proliferation financing possible.

Consult's compliance with the regulatory requirements of FICA contributes to making it more difficult for criminals to hide their illicit proceeds in the formal financial sector and thereby profiting from their criminal activities and cutting off the resources available to terrorists.

FICA incorporates a risk-based approach to compliance elements such as customer due diligence (CDD) into the regulatory framework. A risk-based approach requires Consult to understand its exposure to money laundering, terrorist financing and proliferation financing risks. By understanding and managing the money laundering, terrorist financing and proliferation financing risks, Consult not only protects and maintains the integrity of its business but also contributes to the integrity of the South African financial system.

As a responsible corporate and global citizen; as well as an AI, Consult takes its obligation to play its part in the combating of money laundering, terrorist financing and proliferation financing very seriously.

To this end Consult appreciates and is sincerely thankful for the co-operation and support provided by, and understanding of our financial advisers and their customers, in order to assist Consult to fulfil its obligations in this regard.

5. Definitions

5.1. **"AI" or "AIs"** means Accountable Institution in terms of FICA.

5.2. "**AML/CTF**" means Anti-money laundering and countering the financing of terrorism.

5.3. "**AML Requirements**" means Anti-Money laundering regulatory requirements and include the following legislation:

5.3.1. Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FICA);

5.3.2. Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998) (POCA);

5.3.3. Prevention of Constitutional Democracy against Terrorism and Related Activities Act, 2004 (Act No. 32 of 2004) (POCDATARA);

5.3.4. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended; and

5.3.5. The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended.

5.4. "**Business relationship**" A policy or Investment contract is a long-term business relationship that allows a client to transact with the insurer many times, for example, a recurring fixed-premium investment. However, the take-on of each contract and subsequent trigger events, as described in the RMCP are considered a separate business relationship and therefore requires compliance. Customer Due Diligence (CDD) is not required for subsequent transactions on a specific contract unless any client information has changed or become outdated.

5.5. "**Cash**" is defined in Section 1 of the FIC Act as:

5.5.1. Coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as a medium of exchange in the country of issue; and

5.5.2. Traveler's cheques.

5.5.3. Cash, as defined in the FIC Act, does not include negotiable instruments, transfer of funds by means of bank cheque, bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash.

5.6. "**CDD**" means Customer Due Diligence, and it refers to the knowledge that an AI has about its client and the institution's understanding of the business that the client is conducting with it.

5.7. "**Certified Copy**" for the purposes of this manual means a true copy of the original document which has been certified or commissioned.

5.8. "**Client**" who must be identified, established, and verified means a:

5.8.1. Prospective client who intends on appointing Consult or any one of its financial advisers as its broker on record;

5.8.2. Corporate clients such as companies and trusts;

5.8.3. Controlled and Non-Controlled Clients;

5.8.4. Policyholder or policy owner;

5.8.5. Life insured;

5.8.6. Premium payer;

5.8.7. Beneficiaries (only at claims stage, maturity or payout to beneficiary, beneficiaries on a Trust at new business);

5.8.8. Investment investor;

5.8.9. Cessionary (only if the cessionary is not a known bank);

5.8.10. A natural person acting on behalf of a client (please note that a client can refer to natural persons as well as legal persons); and

5.8.11. A client acting on behalf of another person.

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

5.9.1. Known sexual partners outside the family unit (e.g., girlfriends, boyfriends, mistresses);

5.9.2. Prominent members of the same political party, civil organisation, labor, or employee union as the prominent person;

5.9.3. Business partners or associates, especially those that share (beneficial) ownership of corporate vehicles with the prominent person, or who are otherwise connected (e.g., through joint membership of a company board); and

5.9.4. Any individual who has sole beneficial ownership of a corporate vehicle set up for the actual benefit of the prominent person.

5.10. "**Controlling ownership interest**" refers to the ability by virtue of voting rights attached to shareholdings to take relevant decisions within the legal person and impose those resolutions.

5.11. "**Credible Vendors**" Consult approved vendors that will provide third party electronic validation for natural and legal persons.

5.12. "**CTR**" refers to a cash threshold report submitted in terms of Section 28 of the FIC Act.

5.13. "**CRS**" refers to OECD Common Reporting Standards.

5.14. "**Copy**" includes making a photocopy and taking a digital photograph.

5.15. "**DPIP**" refers to Domestic Prominent Influential Person.

5.16. "**EDD**" refers to Enhanced Due Diligence.

5.17. "**Effective control**" means the ability to materially influence key decisions in relation to a legal person (e.g., the manner in which the majority of voting rights attached to shareholdings are exercised, the appointment of directors of a legal person, decisions taken by a board of directors, key commercial decisions of a legal person), or the ability to take advantage of capital or assets of a legal person.

5.18. **"EFT"** means means a payment instruction carried out by electronic means on behalf of an originator, with a view to making an amount of funds available to a beneficiary, irrespective of whether the originator and the beneficiary are the same person;

5.19. "**Employee**" includes all levels of management, administrative staff, financial advisers, franchise principles, support staff, temporary employees, contractors, and any person directly or indirectly performing a function for or on behalf of Consult.

5.20. "**FATCA**" refers to the Foreign Account Tax Compliance Act.

5.21. "**FATF**" refers to Financial Action Task Force.

5.22. "**FICAA**" refers to the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017).

5.23. "**FIC**" means the Financial Intelligence Centre, the government authority who ensures compliance with the Act and who Consult reports to in terms of the Act.

5.24. "**FIC Guidance Note 3A**" refers to the guidance by the Centre on the practical application of certain client identification and verification requirements.

5.25. "**FIC Guidance Note 7**" refers to guidance on the implementation of various aspects of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued by the FIC on 2 October 2017.

5.26. "**FPPO**" refers to Foreign Prominent Public Officials.

5.27. "**GoAML**" refers to an integrated software solution implemented by the Centre as its preferred platform for registration, reporting, data collection, analysis, and case management.

5.28. "**KYC**" means Know Your Client, in terms of the Financial Intelligence Centre Act (FICA).

5.29. "**ML/TF/PF**" refers to Money laundering, terrorist financing and proliferation financing.

5.30. "**MLTFC Regulations**" refers to Money laundering, terrorist financing and proliferation financing Control Regulations issued under the FICA.

5.31. "**MLCO**" refers to the Money Laundering Compliance Officer.

5.32. "**MLRO**" means the Money Laundering Reporting Officer.

5.33. "**MMH**" means Momentum Metropolitan Holdings Limited and all its subsidiaries.

5.34. "**Consult**" or "**Consult by Momentum**" means Momentum Consult (Pty) Ltd., AI/100831/.

5.35. "**Consult clients**" refers to any natural or legal person who has appointed Consult or any of its representatives as its financial adviser / intermediary.

5.36. "**On-boarding staff**" refers to accountable employees responsible for taking on new financial advisers.

5.37. "**PEP**" refers to a Politically Exposed Person.

5.38. "**PIP**" refers to a Prominent Influential Person. It consists of DPIP, FPPO and Family members or Known Close Associates of DPIP & FPPO.

5.39. "**Product Providers**" refer to the financial institutions with whom Consult has entered into an agreement with as listed in Annexure A and whose products and/or services are offered by one or more Consult financial adviser.

5.40. "**Proliferation financing**" means the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

5.41. "**Property**" in terms of POCA and POCDATARA means money or any other movable, immovable, corporeal or incorporeal thing, and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.

5.42. "**Proceeds of unlawful activities**" means-

5.42.1. any property or any service, advantage, benefit, or reward;

5.42.2. which was derived, received, or retained-

5.42.3. directly or indirectly;

5.42.4. in South Africa or elsewhere;

5.42.5. at any time before or after the commencement of the POC Act; and

5.42.6. In connection with or as a result of any unlawful activity carried on by any person.

5.43. "**Prospective Client**" means a person who approaches Consult to enlist the business' services but has not yet appointed Consult or any of its representatives as their financial adviser.

5.44. "**Representative**" as defined in Section 1 of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS) means any person, including a person employed or mandated by such first-mentioned person, who renders a financial service to a client for or on behalf of a financial services provider, in terms of conditions of employment or any other mandate, but excludes a person rendering clerical, technical, administrative, legal, account or other service in a subsidiary or subordinate capacity. Financial Adviser has a corresponding meaning.

5.45. "**Retail investor**" refers to an individual who purchases securities for his or her own personal account rather than for an organization. Retail investors typically trade in much smaller amounts than institutional investors.

5.46. "**Risk**" means the impact and likelihood of ML/TF/PF/PF taking place. Risk refers to the inherent risk.

5.47. "**Risk based approach**" means an approach whereby Consult identifies, assesses, and understands the ML/TF/PF/PF risk to which it is exposed, and takes AML/CFT measures that are proportionate to those risks.

5.48. "**Risk Management and Compliance Programme**" means the plan developed by Consult which sets out the ML/TF/PF/PF risk identified and the controls to mitigate these risks, and the measures introduced to comply with all other requirements of the FIC Act.

5.49. "**Shell Company**" means a company incorporated in a jurisdiction in which it has no physical presence, and which is unaffiliated with a regulated financial group.

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

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

5.52. "**STR**" refers to a suspicious transaction report made in terms of Section 29 of the FIC Act.

5.53. "**Tipping-Off**" refers to when an employee of Consult discloses information to anyone outside the internal reporting chain as defined in this policy and in so doing the information given could prejudice an investigation into money laundering.

5.54. "**TTR**" refers to a Terrorist Transaction Report made in terms of section 28A of the FIC Act.

5.55. "**Transaction / single transaction**" is a transaction carried out other than in the normal course of business for one of the parties. This includes:

5.55.1. Receiving an instruction or application that will result in a conclusion of a transaction or an alteration to the mandate or an addition of a product;

5.55.2. A trading instruction by a client to buy or sell securities or derivatives;

5.55.3. An amendment or variation of a trading instruction from a client;

5.56. "**Unlawful activity**" means any conduct, which constitutes a crime, or which contravenes any law whether such conduct occurred in the Republic or elsewhere.

6. RMCP Governance

6.1. Identification of Consult

Consult is an entity who carries on the business of a financial services provider requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002).

Consult is registered at the Financial Intelligence Centre, with the FIC Organisational Identity Number: 24022 and Registration number: AI/100831/00012.

In terms of the Financial Advisory and Intermediary Services Act, 2002, ("FAIS"), Consult is an authorised financial services provider and furnishes advice and intermediary services as a regular feature of its business. Consult acts as an intermediary between product providers and clients and is not a product provider in its own right.

Under the provisions of Section 42A of FICAA, Consult has appointed the following Officers-

Anti-Money Laundering Compliance Officer (MLCO)	**Anti-Money Laundering Reporting Officer (MLRO):**
Jacqueline Drotsky	Charlotte Archer
Compliance Officer	AML Operations Specialist
Momentum Consult (Pty) Ltd	Momentum Metropolitan Holdings
268 West Avenue, Centurion, 0157	268 West Avenue, Centurion, 0157
PO Box 7400, Centurion, 0046	PO Box 7400, Centurion, 0046
Tel+ 069 184 5154	Tel 012 673 7348
E-mail: Jackie.drotsky@consultm.co.za	E-mail: charlotte.archer@mmltd.co.za

6.2. Board Responsibility for Oversight of Compliance

6.2.1. The Board of Consult is ultimately responsible for compliance with FICA and the RMCP. All references to compliance made in this RMCP are deemed to be references to compliance with the RMCP. Reference in this RMCP to "the Board" must also be read as meaning the senior management of the business.

The Board and senior management, in addition to their responsibility of managing the business effectively, is also responsible for implementing and reviewing the RMCP on an annual basis and must consider the appropriateness and effectiveness of compliance.

The Board and senior management must also ensure that there are appropriate and effective policies, procedures and controls in place which provide for the Board to meet its obligations relating to compliance review, in particular the Board should:

a) Be fully engaged in decision making processes and take ownership of the risk-based measures adopted since they will be held accountable if the RMCP and RMCP documentation are found to be inadequate.
b) Ensure that it takes into consideration the size, nature, and complexity of the business, including a requirement for sample testing of the effectiveness and adequacy of all its policies, procedures, and controls;
c) Consider whether it would be appropriate to maintain a separate audit function to assess the adequacy and effectiveness of the area of compliance;
d) Ensure that when a review of compliance is discussed by the Board at appropriate intervals, the necessary action is taken to remedy any identified deficiencies;
e) Ensure that Consult, in meeting its obligations, complies with the Regulations and applicable local law which is consistent with the FATF Recommendations; and
f) Provide adequate resources either from within Consult, within the group, or externally to ensure that the AML/CTF/PF policies and requirements are adhered to.

6.2.2. Risk management

a) Undertake ML/TF/PF risk assessments;

b) Establish and implement AML/TF/PF risk frameworks within which to manage Consult's risks; and
c) Develop and implement risk rating models for various business relationships with the relevant supporting due diligence processes.

6.2.3. Governance and oversight

a) Implement appropriate AML/CTF and PF policies;
b) Implement processes for ongoing review and governance of policies;
c) Implement governance structures roles and responsibilities, reporting frameworks and processes; and
d) Managing assurance and regulatory reviews.

6.2.4. People

a) Accountable persons to manage ML/TF and PF risks;
b) Ensure the necessary AML, CTF and PF skilled resources are employed; and
c) Implementation of appropriate AML, CTF and PF training programs.

6.2.5. Process and technology

a) Implement simplified and enhanced CDD measures;
b) CDD programs to meet regulatory requirements whilst remaining customer centric;
c) Establish effective records management practices and processes with supporting systems; and
d) Source appropriate supporting AML/CTF/PF technology solutions and systems.

6.3. Business practice in dealing with cash transactions

a) No employee, contractor or financial adviser acting on behalf of Consult may deal in cash. They are not allowed to receive funds from a client or debtor when establishing a business relationship or facilitating a business transaction;
b) No employee, contractor or financial adviser acting on behalf of Consult may deposit cash or assist in depositing cash on behalf of any client to any product providers bank account; and
c) No employee, contractor or financial adviser may suggest to a client to pay an amount in cash into any product providers bank account.

6.4. Training

In terms of Section 43, Consult must provide training to employees involved in transactions to which FICA applies to enable them to comply with the provisions of FICA and the RMCP. The format of training is not prescribed. Annual FICA awareness training has been designed to raise the level of awareness of employees regarding their obligations under FICA. Records of training attended, and training material are maintained by Consult and/or Human Hub.

The FICA awareness training educates all employees on the following compliance obligations:

a) Establishing and verifying the identity of clients;
b) The duty to keep records;
c) The reporting duties and access to information; and
d) The risk management and compliance program.

The training further enables employees to:

a) correctly identify different types of clients in accordance with the FIC Act;
b) understand the duty to keep records correctly as per Consult's internal procedures; and
c) correctly identify and report different reportable transactions in accordance with the FIC Act.

Consult employees should not be allowed to deal with clients if they have not received training on the FIC Act and RMCP.

Consult's permanent employees' on-going awareness training is provided via Human Hub and TalentLMS for financial advisers and their personal assistants. The RMCP is available on InConsultation, and training records are stored by the High-Performance Learning Centre and Human Hub.

7. Risk-Based Approach (RBA)

The RBA is the most cost-effective and proportionate way to manage ML/TF/PF risks facing any AI and to ensure that measures to prevent or mitigate ML/TF/PF are commensurate with the risks identified.

The RBA requires Consult to understand its inherent and specific exposure to ML/TF/PF risks and to establish a reasonable compliance and risk management programme to manage the risks of AML, TF, and PF, with the intent to protect and maintain the integrity of the South African financial system.

The RBA is not a "zero tolerance" approach as there may be instances where Consult has taken all reasonable measures to identify and mitigate ML/TF/PF risks, but it can still be exploited for ML/TF/PF purposes.

The RBA has, amongst others, the following advantages:

a) It recognises that the ML/TF/PF threat to Consult varies across its client types (natural person, company, trust, etc.) and geographical location;
b) Resources are directed in accordance with priorities, so that the greatest risks receive the highest level of due diligence;
c) If applied correctly, it will improve the efficacy of measures to combat ML/TF/PF while promoting financial inclusion without undermining AML/CTF/PF objectives;
d) It allows Consult to simplify the due diligence measures applied where they assess ML/TF/PF risks to be lower; and
e) Instead of relying on rigid requirements in regulations and exemptions granted, Consult will have greater discretion to determine the appropriate compliance steps to be taken in given instances based on the appropriate ML/TF/PF risk indicators assessed.

The RBA is a systematic approach to risk management and involves:

a) risk identification and assessment – taking account of the client type (natural person, company, trust, etc.), and geographic location (where the client and/or intermediary is resident or incorporated, etc.) to identify the ML/TF/PF risk to Consult;
b) risk mitigation – applying appropriate and effective policies, procedures and controls to manage and mitigate the risks identified;
c) risk monitoring – monitoring the effectiveness of Consult's policies, procedures and controls; and
d) having documented policies, procedures and controls to ensure accountability to the board and senior management.

7.1 ML/TF/PF Risk Assessment

7.1.1 ML/TF/PF Risk Exposure

ML/TF/PF risks are threats and vulnerabilities which puts Consult at risk of being abused to facilitate ML/TF/PF activities. These relate to the potential that clients, by using Consult's services, can exploit Consult to promote ML/TF/PF activities. The nature of these ML/TF/PF risks relate to several aspects such as:

a) the features of the intended target market of clients who are likely to use Consult's services;
b) the geographic locations of Consult's clients;
c) the product types held by Consult's clients;
d) the features and complexity of the client type;
e) the PEP/DPIP/FPPO statuses; and
f) the clients' screening results (adverse media findings, criminal behaviour and sanction lists).

Risk in the context of ML/TF/PF can be thought of as the likelihood and impact of ML/TF/PF activities that could materialise as a result of a combination of threats and vulnerabilities manifesting in Consult as an accountable institution.

Risk rating implies assigning different categories to the various ML/TF/PF risk indicators (client types, product types and geographic locations) according to a risk scale and classifying the ML/TF/PF risks pertaining to different relationships or client engagements in terms of the assigned categories. No two AIs are the same, therefore, the level of risk and the risk ratings attributed to business relationships or other engagements with clients may vary from one AI to another.

The ML/TF/PF risk associated with a particular client engagement does not remain static. Factors underlying any given risk rating will inevitably change over time. It is therefore necessary that Consult re-evaluates the relevance of particular risk factors and the appropriateness of previous risk-ratings from time to time. This is referred to as ongoing CDD.

7.1.2 ML/TF/PF Risk Rating Methodology

MMH implemented a risk rating standard as described in a document entitled "*ORSA Standard Qualitative Risk Rating Methodology Momentum Metropolitan Holdings Ltd*" ("Momentum

Metropolitan ORSA Standard"). Consult, as a subsidiary of the Momentum Metropolitan Holdings Group of Companies, subscribes to this standard when applying its risk ratings to its client base.

The Momentum Metropolitan ORSA Standard is a five-tier rating scale. Consult, as previously stated, is a financial services provider, offering financial products from various product providers (regulated products and services, i.e., collective investment schemes, life insurance products, discretionary and non-discretionary investment products, short-term insurance products, health service benefits), and operates in the Republic of South Africa only.

Consult has therefore concluded that the five-tier rating scale would be the most appropriate risk rating methodology to implement in its environment.

Table 1 below depicts the distribution of the risk exposures that reflect the outcome of this methodology.

Table 1: Momentum Metropolitan ORSA Standard Qualitative Risk Rating Methodology

		Impact				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood		**1**	**2**	**3**	**4**	**5**
Almost Certain	**5**	Medium Low	Medium High	Medium High	High	High
Likely	**4**	Low	Medium Low	Medium High	Medium High	High
Possible	**3**	Low	Medium Low	Medium Low	Medium High	Medium High
Unlikely	**2**	Low	Low	Medium Low	Medium Low	Medium High
Rare	**1**	Low	Low	Low	Low	Medium Low

7.2 ML/TF/PF Risk Indicator Risk Matrices

7.2.1 Process to assess ML/TF/PF risk relating to financial services rendered to the different client types

This is a key risk indicator in the assessment of the overall ML/TF/PF risk as a result of a business relationship entered into with the client.

The five tier ML/TF/PF rating methodology have been developed and have been derived from the MMH ORSA Standard Qualitative Risk Rating Methodology discussed in paragraph 10.2 above.

No.	Legal Structure and Complexity	Weighted Impact Assessment	Likelihood Assessment	Legal Structure and Complexity ML/TF/PF Risk Rating
1	Domestic natural person	Minor	Unlikely	Low
2	Foreign National natural person	Minor	Possible	Medium Low
1	Public Company - Listed on a recognised exchange	Severe	Rare	Medium Low
2	Public Company - Not listed on a recognised exchange	Severe	Likely	High
3	Private Company - Unlisted	Severe	Likely	High
4	State-owned Company - Unlisted	Severe	Likely	High
5	Personal Liability Company - Unlisted	Severe	Likely	High
6	Non-Profit company	Severe	Likely	High
7	Closed Corporations (South Africa)	Severe	Likely	High
8	Partnerships	Severe	Likely	High
9	Trusts	Severe	Likely	High
10	Highly regulated South African entities - Collective Investments Schemes, Retirement Funds and Medical Aid Schemes - Listed	Insignificant	Rare	Low
11	Other entities not mentioned above (i.e., stokvels, churches, clubs, schools, universities, municipalities, cooperatives (associations), etc.)	Severe	Likely	High

The factors identified that will influence the impact rating, and the weight that each factor will contribute in order to determine the overall impact rating for the PEP/DPIP/FPPO status of the client, is indicated in Table 3 below.

Table 3: ML/TF/PF Risk Indicators Relating to the PEP, DPIP or FPPO status (Factors Influencing Impact)

No.	Risk Indicator	Risk Indicator Description	Weighting of Indicator
1	PEP / DPIP / FPPO Status	This indicator considers whether a client with whom it engages to establish a business relationship, or the beneficial owner of that client or immediate family member or known close associate, is either a politically exposed person ("PEP"), foreign prominent public official ("FPPO") or a domestic prominent influential person ("DPIP") which requires enhanced due diligence measures	**100.00%**

Table 4 below provides a summary of the Consult PEP/DPIP/FPPO Statuses and only shows the weighted average of the impact risk assessment of the PEP/DPIP/FPPO status of the client.

Table 4: Consult PEP/DPIP/FPPO Status impact risk assessment

No.	PEP/DPIP/FPPO Status	Weighted Impact Assessment	Likelihood Assessment	PEP/DPIP/FPPO Status Risk Rating
1	Politically Exposed Person (PEP) – South Africa {Preceding 12 months}	Major	Almost certain	High
2	Domestic prominent influential person (DPIP) - South Africa {≤6 Months}	Major	Almost certain	High
3	Domestic prominent influential person (DPIP) - South Africa {>6 Months & preceding 12 Months}	Major	Almost certain	High
4	Foreign prominent public official (FPPO) {Preceding 12 Months}	Major	Almost certain	High

7.3 Process to assess ML/TF/PF risk relating to geographic locations

Should a client reside or be incorporated in a sanctioned country or a high-risk jurisdiction geographic location, the business CANNOT be accepted and must be declined. This is because these geographic locations either appear on the FATF High Risk and other monitored jurisdiction list and/or the geographic locations have sanctions or embargos imposed on them, and/or the geographic location do not subscribe to the combating of ML/TF/PF. Accepting business from a client in one of these geographic locations will expose Consult to severe ML/TF/PF risk. Should

there be merit for an exception to be made such exception must be authorised on a Consult executive level only.

7.4 Process to assess risks relating to adverse findings / criminal behaviour

Table 5 below provides a summary of the Consult Refinitiv World-Check Adverse Findings and only shows the risk assessment of the Refinitiv World-Check findings and Google search in respect of the client.

Table 5: **Consult World-Check Adverse Findings Risk Assessment**

No.	World-Check Findings	World-Check Adverse Findings ML/TF/PF Risk Rating
1	No adverse findings	Low
2	Some findings noted – minor concerns (non-financial sector related)	Medium Low
3	Some findings noted - moderate concerns (financial sector related)	Medium High
4	Adverse findings	High

8. Customer Due Diligence Controls

8.1. Introduction

Previously, Consult was required to establish and verify the identity of a client in accordance with the ML/TF/PF Regulations. The principle of client identification and verification has expanded significantly with the introduction of the obligation to conduct CDD. As a result, the regulations and exemptions relating to client identification and verification have been amended significantly, with most of the regulations having been repealed and exemptions having been withdrawn.

There is no longer a "one-size-fits-all" approach, as the Regulator recognized that this approach will not be appropriate. This is because different industries and/or sectors and businesses within those industries and/or sectors will be exposed to ML/TF/PF risks in differing degrees based on the products and services provided by each business in those industries and/or sectors.

In short, FICA requires Consult to assess the ML/TF/PF risk associated with each business relationship and/or transaction in respect of the unique circumstances and/or services offered by Consult and used by each Consult client.

The Impact of ML/TF/PF Legislation on Consult

The ML/TF/PF requirements are not intended to be unnecessarily intrusive and cumbersome. In fact, ML/TF/PF requirements are intended to be an enhancement to already implemented prudent business practice, and should therefore seamlessly slot into existing processes.

Before engaging in a business relationship with a prospective client, Consult must verify the identity of the client by obtaining FICA verification documents and conducting screening on the client against sanctions, adverse media findings, PEP/FPPO/DPIP, known/suspected criminal behaviour, and any other behaviour/reason which could pose a risk to Consult. Consequently, ML/TF/PF requirements prescribe that:

a) Some additional information/documents must be obtained from the client;
b) Consult must understand the expected business pattern / conduct of the client;
c) All the information collected must be verified;
d) Consult must keep suitable records of the above-mentioned; and
e) Consult must provide specified reports to the Regulator.

8.2. **Establishing a Relationship with a Client**

8.2.1. **New Clients**

Consult cannot establish a business relationship with a client unless the following steps have been taken:

a) To establish and verify the identity of the client ("CDD");
b) If the client is acting on behalf of another person- establish and verify the identity of that other person along with the authority to act on their behalf. For example, an estate late application, curator; and
c) If another person is acting on behalf of the client- to establish and verify the identity of that other person along with the authority from the client to act on their behalf. For example, a discretionary financial services provider, resolution appointing an authorised person to act on behalf of a company, trust etc.

8.2.1.1 Identification of Ultimate Beneficial Ownership

It is of paramount importance that the beneficial owner in respect of the legal person is identified.

Definition of 'beneficial owner' from the Glossary to the FATF Recommendations (24): -

Beneficial owner refers to the natural person(s) who ultimately owns or controls a client and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. To "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

Consult must take reasonable measures in identifying the beneficial owner and measures to verify the identity of the beneficial owner(s), such that it is satisfied that it knows who the beneficial owner(s) is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the client.

Consult must take reasonable measures in identifying direct and indirect ownership and/or control of specific percentage of shares or voting rights; or control over the management and their actions.

Consult needs to:

a) Understand the substance and form of the legal person;
b) Understand the reason for the transaction and SOF, SOW or SOI;
c) Identify individuals behind the institution, not only shareholding, but control; and
d) Ensure that individuals purporting to act on behalf of the entity are authorized to do so.

The lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF/PF by disguising:

a) The identity of known or suspected criminals;
b) The true purpose of a contract held by the legal entity; and
c) The source or use of funds or property associated with the legal entity.

Establishing the identity of the beneficial ownership helps to understand the client's profile to properly assess the ML/TF/PF risks associated with the business relationship, enables Consult to take appropriate steps to mitigate the risks and to collect and gather additional information about the beneficial owners to assist law enforcement efforts.

The standard Beneficial Owner Elimination process to determine who the natural person is, who independently or together with another person, has a controlling ownership interest in the legal person, will be as follows:

a) Consult will consider 25 per cent or more of the shares with voting rights in a legal person as sufficient to exercise control of the legal person. The following will be used to determine the shares with voting rights: organogram, proof of shareholding; independent verification, CIPC etc.;
b) If the ownership interests do not indicate a beneficial owner, or if there is doubt as to whether the person with the controlling ownership interest is the beneficial owner, Consult must establish the natural person who exercises control of the legal person through other means, for example, persons exercising control through voting rights attaching to different classes of shares or through shareholders agreements; and
c) If no natural person can be identified who exercises control through other means, Consult must determine who the natural person is, who exercises control over the management of the legal person, including in the capacity of an executive officer, non-executive director, independent non-executive director, director, or manager.

Once Consult has determined who the beneficial owner of a legal person is, the institution must take reasonable steps to verify that person's identity. Consult will employ the requirements, as per the appropriate checklist to verify the details of the natural person.

8.2.1.2 Beneficiaries of life insurance policies

Consult advisers must ensure that information is obtained in respect of the beneficiaries of life insurance policies, and that the money laundering and terrorist financing (ML/TF) risk associated with the beneficiary must be incorporated into the overall assessment of the ML/TF risk posed by the client.

a) In addition to the CDD measures required to be undertaken in terms of the FIC Act, the RMCP and the compliance checklist, advisers must obtain particulars of the beneficiary of life insurance policies, as soon as soon as it becomes known to the adviser that the beneficiary was designated, or amended by the client;

b) CDD measures in respect of the beneficiary of the policy at onboarding requires that an adviser must apply the same CDD measures as per the relevant FICA CDD checklist based on the type of entity;

c) When a life insurer makes a pay out of a life insurance policy's proceeds, it is entering into a single transaction with the receiver of the funds. The receiver of the funds (beneficiary) becomes the client of the accountable institution, and the resulting FIC Act obligations come into effect;

d) During the due diligence process the adviser may determine that a beneficiary who is a natural person, legal person or a legal arrangement presents a higher ML/TF risk, in which case the adviser should undertake enhanced CDD measures over and above verification on the identity of the beneficiary before the adviser facilitates the actual pay-out of the policy proceeds to the beneficiary;

e) The adviser must take reasonable measures to determine whether the beneficiary and/or, where required, the beneficial owner of the beneficiary is not a person listed pursuant to a targeted financial sanctions list by screening them against the sanction lists on National Treasury's website.

8.2.1.3 Establishing the SOW, SOF, or SOI of the client

Identification of SOW, SOF or SOI for specific transactions is required when Consult concludes the establishment of a business relationship with a client, as to satisfy Consult of the reasonability of establishing a business relationship or single transaction. Consult will require supporting documentation showing the SOW, SOF or SOI for each transaction entered into, as indicated on its Compliance Checklist.

This process is required to enable Consult to establish the identity of the contract owner, as well as the contribution/premium payer on a contract or on a specific transaction, e.g., an ad hoc incoming payment or a single premium investment and is based on the principle that from where/from whom the funds are received (bank account number/s and bank account holder/s) on all transactions is an imperative anti-money-laundering principle.

The identity of a premium payer/contributor needs to be established regardless of whether the case is exempt from other CDD requirements. In a case of an entity, a resolution confirming who may act on behalf of the company will be required.

Note: Consult is obligated to keep record of all bank accounts that are involved in recurring transactions concluded by clients in the course of the business relationship and any single transaction during the full life span of a contract where financial transactions are processed. This

includes proof of payments from where ad hoc/single payments are received and accounts to which withdrawals are paid.

When determining the SOW, Consult should look at the activities that have generated the total net worth of the client, i.e. The activities that produced the client's funds and property.

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

When determining the SOI, Consult should consider the source of the client's regular income.

Consult will, as part of the normal client onboarding process, determine if/what the client's employment status is:

a) Employed (an employee);
b) Unemployed;
c) Self Employed (employer); and
d) Its core business activities and turn-over.

8.2.1.4 Additional due diligence process

Consult's clients entering into low-risk products are excluded from certain requirements as indicated in Annexure M - Compliance Checklist.

If the contribution/premium payer is different from the contract owner/holder Consult must apply the full CDD process to the contribution payer as well. For example, if the policy holder is an individual, but the contribution/premium payer is a legal entity such as a trust or company, the necessary CDD process and documents required as per the specific checklist will also be required for the contribution payer.

a) Identification of an Authorised Representatives of a legal person, trust or natural person

Each natural person that is authorised to transact on behalf of the legal entity must be identified and verified in accordance with the FICA CDD checklists. In addition to the identification and verification requirement to identify each natural person so authorised by the legal person/ trust or natural person, proof of authority must also be obtained.

The legal person may provide the authority in the following manner:

- Power of attorney (in exceptional circumstances and to be approved by Compliance);
- Letter of Authority/ Letter of Executorship;
- Written mandate;
- Resolution duly executed by authorised signatories; and
- Court order authorising the third party to conduct business on behalf of another person.

b) Identification of a sanctioned person or entity in terms of UNSC resolutions

It is vital for Consult to screen its clients to be able to determine whether these clients are sanctioned persons or entities.

In addition, Consult will screen its clients by submitting all client data to the Refinitiv World-Check data base and apply ongoing screening which occurs every night. The Refinitiv sanctions-screening data contains comprehensive coverage of all known sanction bodies and includes more than 280 sanction programs. In addition, they extensively cover narrative or implicit sanctions as well as sectoral sanctions. As Refinitiv records are deduplicated, each subject has a unique record. All information by the sanction issuers is available on that record, together with official sources for verification, this greatly reduces the number of records needing to be screened while assuring quality sanction data. The Refinitiv database enables greater customization and control at name-matching level to screen against specific lists and data sets, or specific fields within those data sets, such as gender, nationality and date of birth.

Refinitiv uses approximate string matching to identify possible matches between word or character strings as entered into the database, it then reduces false positives to a minimum with multiple secondary identifiers in World-Check Risk Intelligence, combined with configurable name matching algorithms and filtering technology, returning only the exact and strong matches based on the rules set by MMH.
If a client does not appear on any of the sanction lists, Consult will proceed with the on-boarding process but if a new client appears on a list, Consult will not proceed with the on-boarding process. Consult is prohibited to continue the relationship with a sanctioned person/entity.

If an existing client appears on a list, Consult has an obligation to follow the Reporting on Property associated with Terrorist and Related activities and financial sanctions pursuant to Resolutions of the United Nations Security Council (Section 28A) process. The matter will also be escalated in accordance with Consult's management process so that an exit process can be initiated.

Consult may not:

- alert the client of the status as sanctioned person/entity;
- acquire, collect or use property of such persons/entity – strictly prohibited;
- transact or process transactions for sanctioned persons/entity; or
- render or provide any financial services to the person or entity – except in instance where Minister of Finance has permitted certain financial services or dealings with the property.

c) Identification of Politically Exposed Person, Domestic Prominent Influential Person and Foreign Prominent Public Officials

Consult must establish if the client falls within this category of clients by screening them against World Check and against sanction lists on National Treasury's website. The table below shows examples of individuals who are or have in the past been entrusted with prominent public functions in a particular country:

Politically Exposed Person ("PEP")	Domestic Prominent Influential Person ("DPIP")	Foreign Prominent Public Officials ("FPPO")	Family members or Known Close Associates of DPIP & FPPO
• Heads of state. • Cabinet ministers. • Members of parliament/local/provincial government. • Senior administrators in government departments (financial departments/tender processes). • Senior judges. • Managers of local municipalities who award tenders. • Senior and/or influential officials. • Ambassador/high commissioner. • Senior representatives of religious organisations.	• President or deputy president. • Government minister or deputy minister. • Premier of a province. • Director-Generals and Chief Financial Officers of government departments. • Member of an executive council of provinces. • Executive mayors and municipal managers • Chief Executive Officers and Chief Financial Officers of state entities like Eskom, Telkom, PRASA, etc. • Judges. • Senior officials of companies that receive certain tenders from government. • A member of a royal family or senior traditional leader.	• Head of state or head of a country or government. • Member of a foreign royal family. • Government minister or equivalent senior politician. • Leader of a political party. • Senior judicial officer. • Senior executive of state-owned companies. • High ranking member of the military/police etc.	• Spouse or civil/life partner. • Previous spouse or civil/life partner. • Children and stepchildren and their spouses or civil/life partners. • Parents. • Siblings and step siblings and their spouses or civil/life partners. • Prominent members of the same political party, civil organisation, labour or employee union as the prominent person. • Business partners or associates who share beneficial ownership of corporate vehicles with the prominent person, or who are otherwise connected e.g., through joint membership of a company board. • Known sexual partners outside

			the family unit (e.g., girlfriends, mistresses and boyfriends). • Any individual who has sole beneficial ownership of a corporate vehicle set up for the actual benefit of the prominent person

The above persons are often susceptible to corruption and bribery and in turn can use their position and influence to launder the proceeds from corrupt activities. Such persons may also use their families or close associates to conceal funds or assets that may have been misappropriated as a result of abuse of their official position or from bribery and corruption. In addition, these persons may also seek to use their influence to gain control of legal entities for similar purposes.

In terms of the FATF standards, and the FIC Amendment Act it is therefore noted that these persons should automatically be classified as a high-risk client. Once it has been established that a client or the beneficial owner of that client falls within one of the above categories Consult will additionally be required to conduct enhanced due diligence measures on an annual basis.

An individual who holds or who is acting in a position for a period exceeding 6 months or has held the position at any time in the preceding 12 months in the Republic, are considered a domestic prominent influential person.

Before Consult is able to enter into any business relationship with these persons the following High-Risk Client On-boarding measures are to be implemented:

PEP/DPIP/FPPO/ High Risk Client On-Boarding Procedure: New clients		
Step	**Name**	**Description**
1	Client Identification	Identify the ultimate client and associated beneficial owner(s) (if not a natural person)
2	Reasonably Established PEP / DPIP / FPPO	If established a PEP/DPIP/FPPO, authorisation must be obtained from the Compliance Manager and CEO of Consult before concluding a transaction or establishing a business relationship. The following precautionary procedures must be followed: • The domestic prominent official must be added to an enhanced ongoing monitoring list; and • The relevant ongoing monitoring activities must be implemented and managed

3	Enhanced Due Diligence	Once supporting documentation has been received, Consult should be able to understand the objective and reasoning for entering into a business relationship with the client
4	CEO & Compliance Approval	PEP/DPIP/FPPO status will be indicated on the relevant application form and submitted to the CEO and the Compliance Manager- if they are comfortable with the level of risk involved, both parties will sign off
5	PEP/DPIP/FPPO Status	The PEP/DPIP/FPPO status will be captured and updated on a relevant database for ongoing monitoring purposes

In the event that an existing client is flagged on the monthly World Check screening as being one of the above-mentioned persons and was not initially designated as being one of them when the relationship was entered into, Compliance notifies the General Manager or Franchise Development Manager who will then be responsible for requesting the necessary enhanced due diligence documentation.

d) Adverse media findings

Consult uses Refinitiv Risk Intelligence Media Check to screen all its clients against any adverse media. The Refinitiv Media Check provides a portal into content from over 13,000 print and web sources, which are carefully selected and continuously vetted for relevance. Media Check structures this content using intelligent tagging to improve screening efficiency and relevancy.

In the event where there is a positive match on the screened client data, Refinitiv will provide links to the detailed media sources. Further searches will be conducted on Google, for all the positive matches to gather more information about the client and confirm the adverse media findings.

Where Refinitiv Risk Intelligence Media Check finds positive matches but cannot provide an accurate confirmation of client identity such as date of birth, client's full names and country of birth an MIE check is conducted on the client to confirm whether the match is indeed positive. Consult's broker appointment form makes provision for consent, signed by the client upon onboarding stage which allows Consult to conduct an MIE check. The MIE results will provide Consult with the following confirmation:

- The identity of the client, including Names, ID number and last known address
- The record of client payment habits over the past 24 months
- Any judgements or court payment orders against the client's name
- Any fraud listing
- Directorship records
- Criminal check
- Trace alerts – red flags against client's names

e) Identification of a refugee/ asylum seeker

During the establishment of a relationship or during the course of the relationship, Consult may rely on the permit issued under Section 22 & 24 of the Refugees Act as an alternative to identify the person should the client not be in possession of official identification documentation. This

document will indicate the names of the refugee, date of birth, thumb print and a bar coded number (used for tracking). The refugee permit has an expiry date, and Consult will not accept expired documents as proof of identity. There is no unique identification number on the permit.

The preferred official identification documentation is as follows:

- Refugee identity document (only valid for two (2) years); and
- United Nations certified travel document.

8.3. Enhanced Due Diligence

a) Certification for EDD Purposes

CDD documentation will not need to be certified. Consult will follow a manual process of verification where a client will be required to provide **copies of verification documents** as per the CDD and Compliance checklists.

However, should there be any unforeseen need or regulatory requirement, documents will be dated and certified within the last three months by a commissioner of oaths located in an equivalent jurisdiction like:

- an embassy;
- a consulate;
- a notary;
- an independent solicitor; and
- barrister /licensed lawyer.

b) Certification by Consult Employees

Consult employees who are commissioners of oath or are suitably qualified and who have sighted the client's original documents may certify copies of the originals.

c) Clarity

The documents must be legible. The photograph of the copy of an identity document must be clear enough to distinguish the features of the client.

d) Contents of the document

Identity documents to verify a Natural Person (RSA citizen) must be a:

- Green barcoded ID;
- Smart Card ID (front and back);
- Valid South African passport containing the following information:
  - Full names;
  - Surname;
  - Gender;

- Birth date;
- Birthplace (Town or country);
- Issue date;
- Expiry date;
- Issuing authority/Issuing country; and
- Passport number.

Birth certificates will only be acceptable for minors younger than 16 years.

For Foreign Nationals:

- United Nations certified travel document/passport;
- Refugee document (valid for 2 years only);
- Valid passport; and
- Valid travel document.

(No temporary identity documents will be accepted).

e) Verification of address

Documents to verify address must adhere to the following:

- Monthly issued document cannot be older than three months (current); and
- If a yearly issued document is used, it must not be older than a year.

The document must show the physical address or ERF number or portion number and township, suburb or town name. In the case of a letter, Consult must confirm that the address provided in the letter matches that as stated in the application. Refer to **CDD checklist** for accepted proof of residential addresses.

Consult advisers may, in exceptional circumstances only, where a client cannot provide verification of their physical address or where the client does not have any residential address verification documents in their own name, complete the declaration of financial adviser section on the CDD checklist, declaring that she/he has visited the client at their residential address.

f) Non-Face-to-Face Clients

Consult must take reasonable steps to confirm the existence of the client and to verify the identity of the natural person/s involved according to the risk associated with the client after applying their information to the Consult risk matrix. There will be specific and adequate measures in place to address the risk involved with non-face-to-face clients that are specific to the business risk framework.

Examples of enhanced CDD measures include (but are not limited to):

- Obtaining additional information on the client;
- Obtaining additional information on the intended nature of the business relationship, and on the reasons for intended or performed transactions; and

- Obtaining information on the SOW, SOF or SOI of the customer.

Scanned and emailed copies of documents may be relevant in instances when client information is obtained in a non-face-to-face situation. In such cases, where enhanced customer due diligence procedures could apply, it implies that documents that are certified as true copies of originals may be accepted, but Consult would have to take additional steps to confirm that the said documents are in fact those of the client in question.

g) Face-to-face Verification

In cases where client information is received in a face-to-face situation, the relevant documents will be sighted as part of the verification process. In a face-to-face meeting, the client is expected to have in their possession copies of their original verification documentation to hand over to the financial adviser.

The below procedure will have to be performed in the event of clients qualifying for Enhanced CDD (High Risk). An annual EDD process is tabled below.

Annual Enhanced Due Diligence Procedure: For Existing PEP/DPIP/FPPO Clients qualifying for Enhanced CDD (High Risk)		
Step	**Name**	**Description**
1	CEO & Compliance Manager signoff	A designated employee should follow an annual review process for PEP/DPIP/FPPOs clients qualifying for Enhanced CDD and to get the CEO and the Compliance Manager's approval and sign off. The review process is to be followed for all existing PEP/DPIP/FPPOs clients qualifying for Enhanced CDD on an annual basis;
2	Review of documentation	FDM/accountable Financial Adviser to request enhanced due diligence documentation to determine if the collected information is consistent with the information currently on record for the PEP/DPIP/FPPOs clients qualifying for Enhanced CDD; and
3	Monitoring of Activities	Monitoring of activities to ensure consistency with documentation on record and profile of PEP/DPIP/FPPOs and High-Risk Clients. If any transaction appears suspicious, to report to Consult's Compliance Officer who will in turn report the suspicious transaction to the Money Laundering Reporting Officer.

Consult's ongoing monitoring process driven by trigger events at appropriate intervals includes the following:

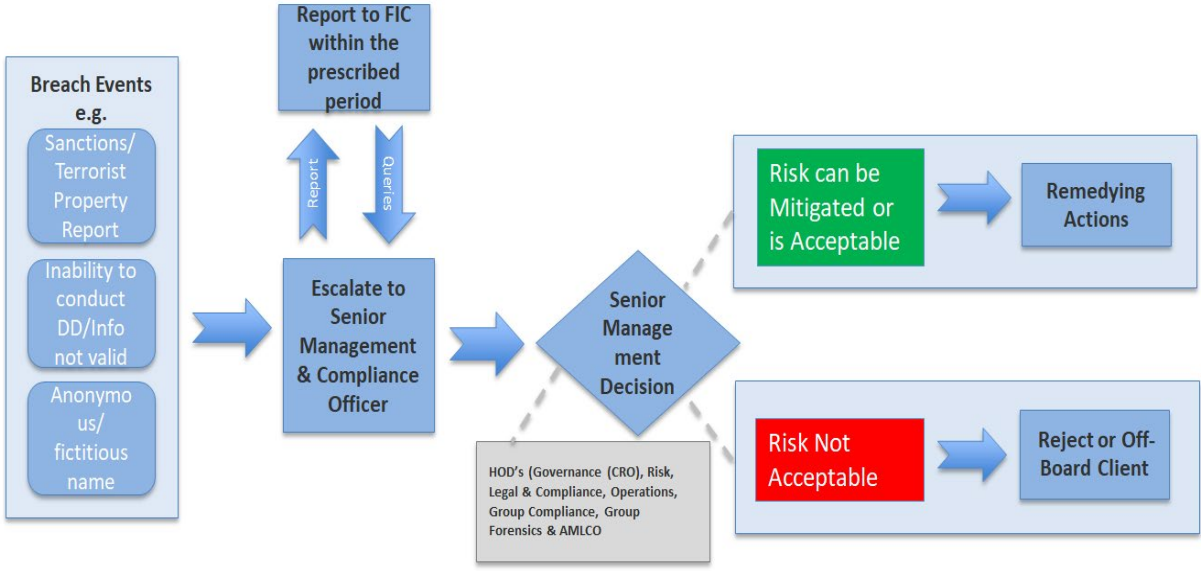
a) Once a trigger event occurs, the client will be taken through the process of risk rating since client's circumstances could have changed over time;
b) The risk matrices (tables 2, 3, 4 and 5) will then be applied to establish the client's new risk rating;
c) If the client's risk rating did not change Consult will continue to process the trigger event;

d) If the client's risk rating has changed to a high or medium-high risk rating, the client will be requested to provide additional documentation necessary to conduct EDD as per CDD checklist;

e) If the additional documentation is acceptable, Consult will proceed with processing the trigger event; and

f) If the additional documentation received is unacceptable to perform EDD, the matter will be escalated to senior management through a breach management process for further consideration.

The below diagram shows **Consult's Breach Management Process**:



8.4. Prohibited Business Relationships

Consult must refuse to enter into a relationship or terminate a relationship, if Consult cannot identify the client and/or the ultimate beneficial owner and/ or the nature of any underlying business.

In particular, Consult is prohibited from entering into/maintain business relationships with individuals or entities known or suspected to be terrorist or a criminal organisation or member of such or listed on any sanction lists.

8.5. Consult Sources of business

It must be noted that Consult sources clients via its financial advisers.

Consult financial advisers are representatives of Momentum Consult (Pty) Ltd, under FSP5503. Consult contracts with financial advisers via a franchise house /financial adviser agreement. As required in terms of FAIS, Consult financial advisers have professional indemnity insurance in place.

A proper due diligence process is undertaken by the Operations Department when financial advisers are onboarded before issuing broker codes. The financial advisers are also monitored on an on-going basis. If there are any persistent or unresolved non-compliance issues it may result in

a code being suspended and/or subsequently blocked. Furthermore, a suspicious transaction/activity will be logged with the FIC through the relevant reporting officer.

8.6. Customer Due Diligence Process

The current process entails that clients' identities are being verified after the business relationship has been entered into. This means that only after the broker appointment and consent form has been signed by the client, the FICA verification documents (as listed in the relevant FICA CDD and Consult's Compliance checklist) and clients' source of funds/source of income/source of wealth are obtained from clients. The clients' profiles are subsequently only created, and the FICA verification documentation uploaded to a Consult approved system within 30 days of the policy/product being incepted.

Consult obtains the client data for screening by extracting a report from the approved system. Screening of the clients can therefore only be conducted once the clients' profiles have been created on the approved systems. This means that Consult screens its clients at least one month after the profiles are created.

Even though Consult obtains the FICA verification documents and conducts the screening against the client after the business relationship has been established, Consult only acts as an intermediary between the client and the product provider and does not receive and/or accepts clients' money into its bank account. The product providers are also responsible for conducting CDD measures on their clients'.

In addition to the above process, Consult financial advisers are obligated to screen their clients against sanction lists on National Treasury's website as part of the onboarding process. The list of sanctioned countries is updated periodically and is available here.

The above processes therefore pose a comparatively lower risk to Consult than it would to a product provider receiving clients' money.

In order to ensure that CDD are not unnecessarily intrusive and cumbersome Consult will strive to, as far as practically possible, impose the least necessary burden on our clients in order to meet our obligations in terms of ML/TF/PF requirements. To this end, Consult intends to over time roll-out and employ the use of:

a) appropriate technology;
b) government issued or controlled sources; and/or
c) reliable 3rd party vendors,

where Consult is confident that it could adequately manage its ML/TF/PF risks.

8.7. Ongoing Customer Due Diligence

Section 21C of FICA provides for ongoing CDD measures. These measures follow on from the obligation to understand the purpose and intended nature of a business relationship.

8.7.1. **Ongoing CDD measures undertaken by Consult include:**

Annual client reviews must be conducted throughout the course of a relationship to ensure that the transactions being conducted in the course of a business relationship are consistent with Consult's knowledge of:

a) the client;
b) the client's business and risk profile, including the source of funds;
c) ensuring that the information that Consult has about a client is still accurate and relevant by obtaining updated verification documentation at least **every two years**;
d) ensuring that screening results are still accurate and relevant by conducting ongoing screening; and
e) re-establishing the source of funds/income/wealth for the client.

The intensity and frequency of ongoing due diligence and/or enhanced due diligence in respect of a client must be determined based on Consult's understanding of any/all risks associated with that client. This means that –

a) Consult obtains specific FICA verification documents based on the type of client, e.g., trust, natural person etc.;
b) Consult screens its entire client database on an ongoing basis; and
c) Consult screens its identified high-risk clients on an enhanced basis, but not less frequently than annually.

9. Screening of employees for competence and integrity and scrutinising of employee information against applicable targeted financial sanctions lists

In terms of FIC Directive 8 of 2023, Consult must screen prospective employees and current employees for competence and integrity, as well as scrutinize employee information against the targeted financial sanctions lists, in order to identify, assess, monitor, mitigate and manage the risk of money laundering, terrorist financing and proliferation financing.

Prior to employing a new employee, Consult must screen the prospective employee for competence and integrity and scrutinize employee information against the targeted financial sanctions lists as an internal control measure aimed at mitigating the risk of Consult being abused by criminals. This must also be done on all current employees periodically for competence, in a risk-based manner.

9.1. Screening for competence refers to determining whether the employee has the necessary skills, knowledge, and expertise to perform their functions effectively. Consult has determined that its Human Resources department will screen prospective and current employees for competence according to its risk-based approach. As part of the screening for competence, Human Resources will consider reviewing the employee's previous employment history, employment references, qualifications, and relevant accreditations.

9.2. Screening for integrity may include determining whether the employee does not have a criminal record, particularly related to crimes of dishonesty, money laundering or other financial crimes. This function will be performed by Group Forensic Services on current employees on an ongoing basis. Human Capital will inform Consult's Compliance Officer of the potential appointment of a new employee, whereby Human Capital will screen the prospective employee for integrity prior to employment.

9.3. In addition to the paragraph above, Consult will implement additional integrity screening measures for employee roles that pose a higher ML/TF/PF risk. Additional screening measures include, but is not limited to, determining whether the employee:

9.3.1. Had conducted themselves in accordance with the generally accepted conduct requirements as applied by Consult;

9.3.2. Held a senior decision-making role in relation to anti-money laundering, terrorist financing or proliferation financing at an accountable institution that was found to have criminally contravened the FIC Act, the Prevention and Combating of Corrupt Activity Act, 2004 (Act 12 of 2004), the Prevention of Organised Crime Act, 1998 (Act 121 of 1998), or the Protection of Constitutional Democracy against Terrorist and Related Activity Act, 2004 (Act 33 of 2004) (POCDATARA Act);

9.3.3. Is a known close associate, or immediate family member of a high-risk client (e.g., high-risk domestic politically exposed persons or foreign politically exposed persons); or

9.3.4. Is a national of a high-risk TF or PF geographic area (refer to PCC 54).

9.4. Not all employees present the same level of ML/TF/PF risk. Consult must therefore determine the level of ML/TF/PF risk an employee role poses and ensure that the screening applied is proportionate to the level of ML/TF/PF risk the employee role presents.

9.5. Where Consult identifies a higher risk of ML/TF/PF based upon the employee role, the accountable institution should apply more stringent competency and integrity screening. To this extend, the CEO, CFO and Compliance Manager who approve the establishment of a business relationship or single transactions with high-risk clients such as domestic politically exposed persons or foreign politically exposed persons and may take decisions which could alter the anti-money laundering, counter terrorist financing and counter proliferation regime of the entity, will be screened more annually, whereas all other employees will be screened every two years.

9.6. Based upon the outcome of the screening of the prospective employee and current employee, Consult will take a risk-based decision to ensure the ML/TF/PF risk is mitigated and managed.

10. Compliance Monitoring

Consult's compliance division conducts compliance monitoring in accordance with its annual monitoring plan which has been approved by Exco.

A monitoring exercise will typically include financial advisers' adherence to their obligations in terms of money laundering legislation and adherence to this policy. Identified compliance breaches are reported to the accountable manager and the breach is addressed with the financial adviser.

The financial adviser is provided with seven days to obtain the outstanding CDD verification documentation.

11. Reporting Obligations and FIC Interventions

The registration and deregistration of accountable and reportable institutions according to schedule 1, 2 and 3 of FICA is intra-group centralized to Momentum Metropolitan Group Forensics Service (GFS). Consult's reporting to the FIC is also centralised to Momentum Metropolitan GFS.

Each respective AI is responsible for the identification, investigation and upon confirmation of a suspicion in a case of suspicious transaction.

11.1. **Inability to conduct customer due diligence (Section 21E)**

Consult must consider submitting a section 29 report to the FIC should they be unable to-

a) Establish and verify the identity of the client and other relevant persons, in terms of their RMCP;
b) Obtain information about the business relationship with the client in terms of their RMCP; and
c) Conduct on going due diligence on the client in terms of its RMCP.

11.2. **Consult's obligation to advise the Centre of clients (Section 27)**

11.2.1. **Natural and Juristic clients**

a) Upon receipt of a Section 27 request from the FIC, via the FIC's go-AML system, which contains the information for the individuals/companies that the enquiry relates to;
b) The MLRO will request the Momentum Metropolitan Group Forensic Services (GFS) to trace any matches or potential matches to existing Consult clients;
c) A template is populated with the information as received from the FIC;
d) This information is then submitted as part of an automated process to look for matches across various product provider platforms;
e) Bank account numbers are not yet part of the existing automated process, but queries are processed on an ad-hoc basis; and

f) The account number provided by the FIC is "run" against the Momentum Metropolitan financial systems (FACS) to establish if Momentum Metropolitan has ever used such an account number. GFS will launch an investigation with the relevant product supplier and/or banking institution if the client does not hold any products with Momentum Metropolitan, for any type of transaction or reason.

Once the interrogation process has been finalized, the MLRO compiles a feedback report to the FIC and submits the report via the FIC go-AML system. The MLRO is required to keep records of submitted files for a period of 5 years.

11.3. Reporting on Property associated with Terrorist and Related activities and financial sanctions pursuant to Resolutions of the United Nations Security Council (Section 28A)

Consult is a financial services provider and does not hold and can therefore not be in possession or have under its control property owned or controlled by or on behalf of, or at the direction of report:

a) Any entity which has committed, or attempted to commit, or facilitated the commission of the financing of terrorism or related activities;
b) A specific entity identified with in a notice by the President; and
c) A sanctioned person or entity identified on the UNSC sanctions list.

The MLRO will implement various checks in an attempt to establish the true identity of the client:

Check: Client's complete portfolio for irregularities, e.g.-

a) Changing/updating of personal information often, especially bank account details;
b) Unexplained ad-hocs & withdrawals, if known to Consult;
c) Attempts for 3rd party payments, if known to Consult; and
d) Incomplete KYC/CDD documents etc., stored on Elite Wealth/MiPortal.

Check: Electronic Systems and Media

a) TransUnion: ITC details (Full names/Address/Contact details/Occupation etc.);
b) Experian: ITC details ((Full names/Address/Contact details/Occupation etc.);
c) Google: Fraud/corruption & general search;
d) World Check: Searches for clients on https://sanctionssearch.ofac.treas.gov/. If the client is in any way high-risk/politically exposed their information will come up on this search and details will be provided regarding why they are high-risk/politically exposed, and
e) Windeed: Provides details of companies that the client is/was a member of.

Once the MLRO has finalised the investigation and has managed to reach a conclusion, the MLRO, will be in a position to provide comments on KR1S and make an educated decision in determining if the client is a terrorist or assisting in terrorist funding.

If the client or entity has been identified as a terrorist or is assisting in terrorist funding, the MLRO is to immediately freeze all assets in the name of the client and immediately inform the FIC of the client's status.

Business must be informed that NO withdrawals are permitted from any contracts in the name of the client.

A warning message will be placed on system informing business that NO withdrawals are permitted without referring the contract to the MLRO.

The MLRO keeps record of all cases which are reported to the FIC. These contracts are to be monitored monthly, to ensure that no unauthorised payments are processed.

11.4. **PEP/DPIP/FPPO ("PIP")**

Consult obtains the information from the relevant FICA CDD checklist or from the product supplier application form where such application form contains the PEP, DPIP or FPPO declaration section. WorldCheck screening will be conducted over and above the client declaration.

11.4.1. **PEP/DPIP/FPPO Business Rule Principles**

Overarching principles

a) Once a client is identified as a PEP/DPIP/FPPO, they will always remain a PEP/DPIP/FPPO;
b) If any one of the directors or members of a Juristic entity is a PEP/DPIP/FPPO, then the Juristic will be classified as a PEP / PIP; and
c) The WorldCheck screening results of the individual directors / members of the juristic entity must be linked to the Juristic, meaning if the Juristic entity is a negative match, but for individual members a match could be found, then the juristic entity receives a positive match.

Outcome from the World check search

a) No match found; business process may continue as usual;
b) If possible positive matches (true or false) are found, the client must undergo further investigation;
c) Where true positive matches are identified, the Compliance Manager and the CEO must sign off on the screening report, indicating whether the client may remain on Consult's books.

Outcome from the Sanction list search:

a) No results found; business to continue with the client relationship;
b) One or many possible positive matches – The business process is to establish whether any of the possible results are at least a 70% match with the details Consult has about the client;
c) A positive result will be escalated to GFS; and
d) A positive match on the sanctions list could result in the termination of the business relationship.

11.5. **Cash threshold reporting**

Consult does not receive cash deposits or payments into its bank account and section 28 (Cash transactions above prescribed limit) reporting therefore does not apply to Consult.

11.6. **Reporting of Suspicious and Unusual transactions: STRs (Section 29)**

The FIC Act applies to any person identified in Schedule 1 and Schedule 3 to the FIC Act.

Any person associated with Consult as the owner, a manager or employee of Consult, is subject to the obligation to report suspicious or unusual transactions and activities to the Centre.

The obligation to report in terms of section 29 of the FIC Act arises when-

a) he or she becomes aware of something; or

b) circumstances arise in which a person can reasonably be expected to be aware of something; or

c) circumstances arise in which a person can reasonably be expected to suspect something.

This means that a person associated with a business, as described above, must report his or her knowledge or suspicion to the Centre.

Section 29(1) of the FIC Act describes the "something" referred to above as situations concerning the business itself; or concerning transactions or potential transactions to which the business is a party; or concerning an activity which may lead to the business being abused by money launderers.

The "something" also relates to:

a) the proceeds of unlawful activity;
b) unlawful activity;
c) facilitating the transfer of proceeds of unlawful activity;
d) has no apparent business or lawful purpose;
e) may be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax;
f) an offence relating to the financing of terrorist and related activities;
g) an offence relating to proliferation financing activities;
h) the contravention of a prohibition under section 26B of the FIC Act; and / or
i) any structuring of a transaction or activity which is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act;

It is important to note that section 29 of the FIC Act refers to reports being made in connection with suspicions concerning the proceeds of unlawful activities and money laundering, terrorist financing, proliferation financing and financial sanctions offences as opposed to criminal activity in general. The FIC Act therefore does not require reports to be made on suspected crimes or unlawful conduct by a person (apart from money laundering, terrorist financing, proliferation financing and financial sanction activities).

Examples of deemed Suspicious Transaction:

a) New business or existing business relationship, where the proper identification of client/s cannot be established, or information related to the identification and verification process is suspicious;
b) Where a financial adviser or employee facilitating a transaction actually knows, or believes that there is a reasonable possibility that the client's/clients' name/s is/are false;
c) Where the client transfers ownership or cedes a contract to a party outside the borders of the RSA, or to a non-resident, or to a non-citizen;
d) Application for a policy from a potential client in a distant place where a comparable contract could be provided "closer to home;"
e) Application for business outside the policyholder's normal pattern of business;
f) Any transaction or suspicious transaction that involves an undisclosed party;
g) Early termination of a product, especially at a loss caused by front-end loading of costs, or where cash was tendered and/or the refund is to a third party;
h) The transfer of the benefit of a product to an apparently unrelated third party (e.g., outright cessions);
i) Requests for a large purchase of a lump-sum contract where the policyholder's history shows small, regular payment contracts;
j) Attempts to use third-party funding to purchase a policy;
k) The applicant shows no concern for the performance of the policy but much concern for the early cancellation of the contract;
l) The applicant attempts to use cash to complete a proposed transaction when other payment instruments would normally be used in this type of business transaction;
m) The applicant requests to make a lump-sum payment by a wire transfer or in foreign currency;
n) The applicant appears to have policies with several institutions; and
o) The applicant purchases policies in amounts considered beyond the client's apparent affordability.

A person who files a report in terms of section 29 of the FIC Act, should evaluate matters concerning both the reporter's internal business and the business of the client, or potential client in question and the transactions involving the business, in relation to what seems appropriate and is within normal practices in the particular line of business of that person or entity type, and bring to bear on these factors such as the knowledge the reporter may have of the client. This should involve an application of the person's knowledge of the customer's business, financial history, background, and behaviour.

A particular category of transactions that are reportable under section 29(1) of the FIC Act are transactions which a person knows or suspects to have no apparent business or lawful purpose. This refers to situations where customers enter into transactions that appear unusual in a business context or where it is not clear that the purpose of the transaction(s) is lawful. In order to identify situations where customers wish to engage in these unusual transactions a person would have to have some background information as to the purpose of a transaction and evaluate this against several factors such as the size and complexity of the transaction, as well as the person's knowledge of the customer's business, financial history, background, and behaviour.

Process:

Once a suspicious transaction has been identified, the employee must immediately inform the MLCO.

a) The MLCO will discuss and review the matter;
b) Where appropriate, additional information must be provided relating to the client or transaction if it is relevant to the matter under consideration;
c) If an employee suspects the Head of the Business Unit, to be involved with the suspicious activity under consideration, the MLCO should be contacted immediately;
d) Suspicions must not be discussed with anyone other than direct management, and the Momentum Metropolitan Group MLCO. It is of vital importance, regardless of whether the suspicions are proven true or not, that no mention of these suspicions be made to the client;
e) Any discussion of this nature would be deemed as "tipping-off," which is a criminal offence;
f) Employees should always neither confirm nor deny the existence of a report to the client or to a third party;
g) Any correspondence that could indicate the existence of a report should not be placed in the client's file;
h) The matter will be reported to the MLRO, who will prepare the section 29(1) report for review by Consult's MLRO, who in turn will acknowledge its receipt in writing or ratification;
i) The employee will then receive guidance from the MLRO on how to proceed with the client in question;
j) If the client demands that subsequent transactions be executed, the situation must be discussed with the MLRO before any action is taken;
k) In certain cases, the Momentum Metropolitan MLCO may decide to allow transactions to continue in order not to raise the client's suspicions. Regardless, the Momentum Metropolitan Group MLCO should be kept informed of all subsequent dealings with the client;
l) The process is handled exclusively by the Momentum Metropolitan Group MLCO;
m) The Momentum Metropolitan Group MLCO must judge, based on the employee's report and all available information (including additional enquiries), whether or not the transaction has remained suspicious;
n) If the Momentum Metropolitan Group MLCO judges that the transaction has remained suspicious, the MLRO will make an official report to the FIC via the go-AML system;
o) All reports made to the FIC must be stored manually and electronically by the MLRO;
p) The initiating employee will receive an acknowledgment of the receipt of report, from the MLRO confirming that their personal legal obligations in terms of this policy have been met;
q) Once the report has been submitted, the FIC will respond to the submitted report by issuing an "Approval or Rejection" report;
r) If the report is approved, the Approval report must be stored electronically and manually;
s) If the report was rejected, the MLRO must investigate the reason for the failure and correct the report within 48 hours (2 business days) before re-submitting the report for approval;
t) The MLRO must store all responses received as hardcopies and electronically for a minimum period of five years; and
u) The MLRO only has 14 business days to ensure that all reports are downloaded and stored, before the FIC moves the response to an archived status, after which the report can no longer be accessed or downloaded.

11.7. Consult does not transfer money to and from the Republic of South Africa, therefore Section 31 reporting does not apply to Consult

11.8. Reporting procedures and furnishing of additional information (Section 32)

11.9. Requests for information in terms of section 32 of the FIC Act provide the FIC with a mechanism to obtain additional information concerning a report submitted by Consult, including the grounds for the report.

Process

a) The MLRO receives a Section 32 request on the go-AML Message Board in Consult's name.
b) The MLRO must without delay provide the requested detail and documents to the FIC by submitting an Additional Information File (AIF) or an Additional Information File Transaction Report (AIFT) report;
c) All information must be provided as per the Section 32 request within the given time frame;
d) All AIF/AIFT reports submitted to the FIC must be stored manually and electronically;
e) This includes the Rejection/Accepted reports received from the FIC, after a report has been submitted;
f) All requests received from the FIC contains a reference code, this is the only reference code which must be used when providing feedback to the FIC on a specific request; and
g) All Rejected reports must be corrected and resubmitted, within 48 hours of being rejected, until the report has been accepted.

11.10. **Intervention by the Centre (Section 34)**

The FIC may direct Consult in writing not to proceed with a specific action as detailed in the Section 34 request. This can include but is not limited to the facilitation of a specified transaction or proposed transaction for a period not longer than 10 days. For the purposes of calculating the period of 10 days, Saturdays, Sundays and proclaimed public holidays are excluded.

This intervention enables the FIC to make the necessary inquiries concerning the transaction and if the Centre considers it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions regarding the transaction.

Process

a) The MLRO will receive a Section 34 request, on the go-AML Message Board, in Consult's name;
b) The MLRO must without delay act upon the instruction received from the FIC
c) The MLRO will inform Consult's MLCO accordingly;
d) Senior Management must be informed of the Section 34 request received on a transaction/client/entity/contract/policy;
e) Senior Management must, in collaboration with the financial adviser, provide ongoing monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed;

f) The MLCO must report any additional relevant information with regards to any change in client behaviour or any further information received or established to the MLRO;
g) Once the said 10 days have expired, without further instruction from the FIC, it is suggested that the MLRO enquire further instruction from the FIC, via Consult's go-AML Message Board, to ensure that no unauthorized transactions are processed;
h) All requests received from the FIC contains a reference code, this is the only reference code which must be used when providing feedback to the FIC on a specific request; and
i) All communication and reports submitted to the FIC must be stored manually and electronically for a period of 5 years.

It is important to note that the requests in terms of sections 32 and 34 above may also be addressed to Consult in different manners, and it is therefore imperative that employees are aware of their responsibilities in terms of the Momentum Metropolitan Dawn Raid Policy; attached hereto as Annexure L.

11.11. Power of access by authorised representatives to records in respect of reports required to be submitted to the FIC

The FIC may request information from Consult or-

a) A specified person or entity that is or has been a client of Consult;
b) A specified person acting or has acted on behalf of any client of Consult;
c) A client of Consult or person is acting or has acted for a specified person;
d) Request Consult to allocate the reference number etc. specified by the FIC to a person with whom Consult has had a business relationship; and
e) The type and status of a business relationship with a client of Consult.

Process

a) If a person claiming to be a representative of the FIC insists on access to any records held by Consult, Consult employees must refer the request for information to the MLCO for further attention;
b) If the FIC should ask Consult for access to its records, they must never inform any other person of this request or of the nature of the records sought by the FIC, except to inform the MLCO. (If an employee does, it may be regarded as 'tipping off' which is a criminal offence);
c) The MLCO will inform the MLRO and GFS of the request for information from the FIC;
d) The MLRO/GFS will ensure that the representative from the FIC has written authority to represent the FIC and a warrant to gain access to the records;
e) In the event that a printout of the electronic records of Consult is made and provided to a representative of the FIC (or the police), a Commissioner of Oaths will certify that the printout is an extract copy of Consult's electronic records; and
f) The MLCO and MLRO will keep a record of all requests for information from the FIC, manually and electronically for a period of five years.

11.12. Confidentiality

All staff must satisfy any legal obligation to report knowledge or suspicions relating to the proceeds of unlawful activities or money laundering i.e., in the required format and within the time frames required. Where a suspicious activity report has been filed or otherwise reported to the MLCO and MLRO, staff must not notify any person of any matters relating thereto i.e., besides the MLCO and MLRO or specifically authorised Consult officials. All reports submitted remain confidential and each employee is protected. Consult and its employees can rely on the protection provided by Section 38 of FICA and Section 7A of POCA.

Under no circumstances must the person suspected of money laundering be alerted to the report or must the matter be discussed with anyone except the MLRO the MLCO and management. Consult has introduced training to minimize the risk of an employee "tipping off" a client or any other person with whom they come into contact. A person found guilty of "tipping-off" and acting negligently constitutes a fine of up to R10 million and/or 15 years imprisonment.

12. Record Keeping

Record keeping is an essential and required process which successfully enables Consult to combat money laundering, terrorist financing and proliferation financing. The records of client identities and transaction activities are of paramount importance as these records can be used as documentary evidence which can assist law enforcement authorities in the detection, investigation, prosecution, and the repossession of criminal funds where illegal flow of funds is concerned.

In this regard all interaction with clients, whether directly or through a person acting on behalf of a client would require that Consult obtains all relevant CDD documentation.

12.1. **Duty to Keep Records**

The duty to keep records arises whenever we establish a business relationship or conclude a single transaction with such a client. FICA requires Consult to keep records of the following:

a) Copies of proof of identification documentation;
b) Copies of proof of residential address;
c) Copies of proof of source of funding. e.g., bank statement;
d) Documentation which proves nature of business relationship or occupation; and
e) Verification documents and any other information collected about the client e.g., all information linked to a transaction e.g., dates, values, parties involved, bank accounts etc.

12.2. **Period for which records must be kept**

Consult has an obligation to retain records for the following period:

a) Records relating to establishment of the business relationship must be kept for at least five years from date of termination of business relationship;
b) Records relating to all transaction must be kept for at least five years from the date which the transaction was concluded;

c) Records relating to a transaction or activity which gave rise to reporting a suspicious activity or transaction to FIC must be retained for at least five years from the date which a suspicious activity or transaction was reported to the FIC;
d) Records which Consult has in its possession which is connected to an ongoing investigation must be kept until such time that relevant law enforcement authority has confirmed that the case has been closed; and
e) Records not being used for the intention for which it was collected must be immediately destroyed.

12.3. **Record keeping methods**

Records may be kept by way of storing original documents or copies of original documents, scanned versions of originals in electronic format in an effort to reduce the density of such records and must be kept on the system provided by Consult for record keeping purposes.

Consult financial advisers may store all original documents in their offices, provided that such documents are kept safe from destruction and unauthorised access.

12.3.1. **Electronic storage**

a) All documents must be scanned onto the relevant recordkeeping systems;
b) Electronically retained records can be reproduced in a legible format. These electronic records are secured by unique User IDs, passwords etc.;
c) Consult must inform clients of its intention to retain the client's records with a specific third party and must seek the clients consent in sharing their personal information with this third party; and
d) Consult must safeguard and ensure that there are controls in place such as firewalls that will safeguard against anyone tampering with the electronic data. Other preventative measures are as follows, user logs, network logs, password-controlled access, levels of authority etc.

12.4. **Consult must ensure that the following principles are met:**

a) It has easy free access to the records and will have the records readily available to the FIC and relevant supervisory body as and when it is needed;
b) The liability remains with Consult should the third party fail to comply with the provisions of this Act;
c) Consult provides the FIC and supervisory bodies with the full particulars of the third party;
d) Electronically retained records can be reproduced in a legible format;
e) Consult will inform clients of its intention to retain the client's records with a specific third party and will seek the clients consent in sharing their personal information with this third party; and
f) Consult will safeguard and ensure that there are controls in place such as firewalls that will safeguard against anyone tampering with the electronic data.

12.5. Consult will store the records in a detailed manner which will enable easy identification of such records.

12.6. Consult will take reasonable steps to maintain the correctness of particulars of clients, which are susceptible to change.

12.7. Based on the risk-based approach it is recommended that Consult should verify particulars of clients, at any stage when Consult interacts with the client.

12.8. Consult will ensure that records are tamper proof and that there are safeguards in place to prevent the unauthorised access to information stored electronically.

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

IMPORTANT NOTE: Consult remains responsible for compliance with its obligations in terms of the FIC Act and the FIC Amendment Act.

Consult may rely on the services of a third party or the relevant product provider to perform activities relating to the establishing, verifying and validation of clients' CDD documents to establish and verify the identity of their clients, and for record-keeping purposes as required in terms of the FIC Act and the Regulations to the FIC Act. However, Consult remains liable for compliance failures associated with and/or caused by such arrangement.

13. Non-Compliance

Any contravention of the principles and processes contained in the RMCP or of the FIC Act will be dealt with in accordance with the disciplinary procedures as set out in the financial adviser agreement, franchise house agreement and the Practice Note on Financial Planning and Advice.

Any person convicted of an offence in terms of Chapter 4 of FICA may be liable to imprisonment for a period of not more than 15 years or a fine of not exceeding R 100 000 000.

Please refer to table below for further information pertaining to the offences and penalties associated with the FIC Act. Consult reserves the right to recover any penalty imposed upon it by a Regulator due to the negligence by an employee.

The table below shows Penalties for Non-Compliances

Compliance Duty		Sections of the FICAA	Regulations	Administrative Sanction / Fines	Criminal Sanction
Section 46: Failure to identify persons		21(1), 21(1A)	3, 5, 7, 9, 11, 15 and 17(1)	Natural Person = R10 million Legal Person = R50 million	
Section 46A: Failure to comply with duty in regard to customer due diligence		21A to 21H		Natural Person = R10 million Legal Person = R50 million	
Failure to verify particulars			3, 5, 7, 9, 11, 15 and 17(1) in accordance with regulations 4, 6, 8, 10, 12, 14, 16, and	Fine not exceeding R1 million	Imprisonment not exceeding 3 years
Record Keeping		21(1), 22A(1) and (2), 23, 24(1) and 24(3)	Chapter 2	Natural Person = R10 million Legal Person = R50 million	N/A
Reporting	**CTR**	28	22, 22B, 22C & 24	Natural Person = R10 million Legal Person = R50 million	15 years or R100 million
	TPR	28A(1) to 28A(3)	22, 22A, 23B, 23C & 24		
	STR	29(1) and (2)	22, 23, 23A & 24	N/A	
Failure to implement Risk Management & Compliance Programme		42	25, 26, 27	Natural Person = R10 million Legal Person = R50 million	N/A
Failure to comply with duty in regard to Governance		42A(1) to (4)	N/A	Natural Person = R10 million Legal Person = R50 million	N/A
Failure to provide training (or appoint Compliance Officer)		43(a) and (b)	N/A	Natural Person = R10 million Legal Person = R50 million	N/A
Failure to register with the Centre		43B	27A	Natural Person = R10 million Legal Person = R50 million	N/A
Failure to comply with directives of Centre or Supervisory Body		43A(3) and 45C(3)		Natural Person = R10 million Legal Person = R50 million	N/A
Unauthorised access to computer system, application or data		65(1) and (2)		A fine not exceeding R10 million	Imprisonment not exceeding 5 years
Failure to comply with Regulations		77	29	Fine not exceeding R1 million	Imprisonment not exceeding 3 years

14. Protection of personal information

14.1. **Introduction**

In order for Consult to comply with the FIC Act obligations, it is required to obtain, process and further process certain necessary personal information and special personal information.

The South African data privacy legislation is the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPI Act). The POPI Act promotes the protection of personal information and special personal information processed by public and private bodies and sets conditions for obtaining, using and processing of such information.

The FIC Act applies in a mutually non-conflicting manner to the principles of the POPI Act. The FIC Act provides the necessary justification in law that accountable institutions and reporting institutions require to obtain, process and further process relevant personal information and special personal information in terms of the POPI Act.

14.2. **Risk based approach**

The personal information and special personal information obtained by Consult about the client in terms of the FIC Act should be adequate, accurate, relevant, up to date and proportionate to the ML/TF/PF risk level, for the purposes of complying with the obligations of the FIC Act, taking into account section 38 of the POPI Act.

Where Consult obtains personal information and special personal information, that is not required and not necessary to achieve the purposes of the FIC Act, and which is not proportionate to the ML/TF/PF risk, this would amount to an excessive collection of information which is not aligned to the principles of data privacy. The harmony between the application of the FIC Act and the POPI Act lies in, and is achieved by, Consult asking only for personal information and special personal information that is necessary to achieve the purposes of the FIC Act.

14.3. **Customer due diligence**

Upon establishing a business relationship or conducting a single transaction when collecting personal information or special personal information, Consult must inform or disclose to the client, that it must comply with its obligations in terms of the FIC Act. In order to do so it has to obtain, use and further process certain personal information and special personal information.

Once Consult has obtained the information for purposes as set out in the FIC Act, it may then use that personal information and special personal information for processing and further processing to comply with their obligations in terms of the FIC Act.

Clients have the freedom to choose whether to establish or continue with a business relationship with Consult. Consult may advise a client on the consequences should the client refuse to provide personal information or special personal information, provided such information does not amount to tipping off.

Where the client does establish or opts to continue with a business relationship, Consult must comply with its obligations in terms of the FIC Act. Where the client refuses to provide personal information or special personal information as required for purposes of complying with the FIC Act and bases the refusal on data privacy concerns or laws, Consult:

a) May not establish a business relationship or conduct a single transaction with a client;
b) May not perform any act to give effect to a single transaction;
c) Must terminate an existing business relationship with a client in accordance with Consult's risk management and compliance programme (RMCP), and
d) Consider filing a report in terms of section 29 of the FIC Act.

Where Consult follows an approach of single client view, it is recommended that the client be notified that their information may be shared across the MMH Group of Companies.

14.4. **Reporting**

Conducting certain obligations in terms of the FIC Act amounts to processing in terms of the POPI Act which includes, but is not limited to, filing of FIC Act section 28, 28A and 29 regulatory reports with the Centre. The filing of reports as processing of personal information and special personal information is justified as it is an obligation imposed by the FIC Act.

Consult may not disclose information relating to a regulatory report filed with the Centre in terms of section 29 of the FIC Act (unless as provided for in law). Further, Consult and its employees may not disclose information relating to requests for information in terms of section 27 and section 32 of the FIC Act.

Disclosing that a regulatory report was submitted to the Centre in terms of section 29 of the FIC Act, or the content of such a report other than as provided in terms of the FIC Act is regarded as a tipping off offence in terms of the FIC Act (section 29(4)).

Consult can collect personal information and special personal information from a third party where compliance with the requirement to collect directly from the client or other persons would prejudice the lawful purpose of the collection. There is justification for Consult to obtain such further information from a third party and not directly from the client or other person, as the collection of information directly from the client may amount to tipping off.

14.5. **Record keeping**

Records of personal information and special personal information being kept by Consult or a third party on behalf of Consult must be held for the purposes of combating money laundering,

terrorist financing and proliferation financing, in accordance with the FIC Act, the Money Laundering Terrorist Financing Regulations and Consult's RMCP.

Where the period, as set out in the FIC Act and Consult's RMCP lapses, the personal information and special personal information may not be used for purposes of the FIC Act.

14.6. Use of third parties

Consult can either obtain personal information or special personal information directly from the client or through the use of a third party. Where Consult does obtain personal information or special personal information from a third party, it will disclose to the client that it relies on third parties for obtaining certain personal information and special personal information.

14.7. Conclusion

The client's information is used for the effective rendering of financial services to the client and to ensure the suitability of advice. Consult will take all reasonable steps necessary to secure the integrity of any personal information which it holds about its clients and to safeguard it against unauthorized access.

Clients may write to us to obtain a copy of the information Consult has on record about them. Consult maintains relevant documents for a period of five years after the business relationship is terminated, as required by the FIC Act.

15. Annexures

15.1. **Annexure A – Consult List of Product Providers**

15.2. **Annexure B – Client Onboarding process**

15.3. **Annexure C – Financial Adviser onboarding process**

15.4. **Annexure D – FICA CDD Checklist for Natural persons or Sole Proprietors**

15.5. **Annexure E – FICA CDD Checklist for Private Companies**

15.6. **Annexure F – FICA CDD Checklist for Listed Companies**

15.7. **Annexure G – FICA CDD Checklist for Close Corporations**

15.8. **Annexure H – FICA CDD Checklist for Trusts**

15.9. **Annexure I – FICA CDD Checklist for other legal persons**

15.10. **Annexure J – FICA CDD Checklist for Partnerships**

15.11. **Annexure K – FICA CDD Checklist for Foreign Companies**

15.12. **Annexure L – Dawn Raid Policy**

15.13. **Annexure M – Compliance Checklist**