Financial
Intelligence Centre

ASSESSMENT OF THE INHERENT MONEY LAUNDERING AND TERRORIST FINANCING RISKS

ACCOUNTANTS

November 2023

CONTENTS

1. INTRODUCTION

1.1 Money laundering can be described as the process whereby criminals attempt to conceal the proceeds of their criminal activities from the actual crime, thereby giving the funds derived from criminal activities an appearance of legitimacy.

1.2 Terrorist financing is the process by which individual terrorist and terrorist organisations obtain funds to commit acts of terrorism.

1.3 The Financial Action Task Force (FATF) define designated non-financial businesses and professions (DNFPBs) – which includes accountants – as "sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures".

1.4 FATF's Guidance for a risk-based Approach for the Accounting Profession published in 2019[1] states in the cover webpage to this guidance the following: "The legally required services that accountants provide make them vulnerable to become unwittingly involved or accessory to money laundering or terrorist financing activities. Recent FATF research highlighted examples of accountants that had used their occupation, business infrastructure and knowledge to facilitate money laundering for criminal clients. For example, professional money launderers have been known to keep a shadow accounting system with records of transactions involving proceeds of crime. Accounting and related auditing firms must therefore protect themselves from misuse by criminals and terrorists."

1.5 The FATF then in the cover webpage provides its expectation regarding accountants as designated in the FATF Standards, in the following terms:

"The accounting sector must meet customer due diligence and record-keeping requirements when, on behalf of their client, they are involved in real estate transactions; managing money, securities or other assets; managing bank, savings

[1] See the link - FATF Guidance for a Risk-Based Approach for the Accounting Profession (fatf-gafi.org).

or securities accounts; creating, operating or managing companies, or legal persons and arrangements and buying and selling business entities."

1.6 The 2019 FATF Guidance for a risk-based approach for the accountancy profession requires AML/CFT supervisors of "professional accountants in public practice (also referred to as "accountants" or "accountancy profession") to "identify, assess, and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed." This sector is regarded as potentially highly vulnerable for ML/TF.

1.7 The Financial Intelligence Centre (FIC) is conducting a sector risk assessment of the inherent ML/TF risks of accountants in South Africa, and this draft risk assessment for accountants addresses the ML/TF risks to which accountants in South Africa may be exposed and aims to assist accountants and accountancy institutions providing such services in identifying such ML/TF risks and introducing measures to mitigate and manage these identified risks.

1.8 The purpose of this risk assessment is to identify the known or expected inherent risks of ML/TF for accountancy profession in South Africa resulting from the threats it faces, and its vulnerabilities, and consequent ML/TF risks. In this regard, it should be understood that accountancy services remain attractive to criminals and terrorists due to the ability to use the respectable services of accountants to gain legitimacy or transfer value related to the proceeds of unlawful activities as well lawful activities aimed at terror financing. This is because accountants are well positioned and skilled to legitimise transactions through accountancy practices.

1.9 This draft sector risk assessment is informed by the FATF Recommendation and Methodology and related guidance and best practice documents, developing best practice on assessed risks in the accountancy profession issued by national authorities and supervisory competent authorities in other jurisdictions, and open-source information on the inherent national and international money laundering and terrorist financing risks of accountants in South Africa.

2. SCOPE, LIMITATIONS AND METHODOLOGY OF THE RISK ASSESSMENT

2.1 This sector risk assessment report addresses principally the inherent ML/TF risk factors facing accountants in South Africa pertaining to products, services, clients, transactions, delivery channels and geographical areas, and the potential mitigation of these risks by complying with the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act). The reference to accountants in this document applies to professional accountants and in particular those individuals and institutions that are providing the services to trusts and companies in terms of item 2 of Schedule 1 of the FIC Act.

2.2 Although it is recognised that these risks could be mitigated by introducing processes and procedures in accordance with the requirements of the FIC Act, details of such mitigation factors were not included in this report. The report focuses on inherent risks.

3. SECTOR OVERVIEW AND FIC ACT LEGISLATIVE FRAMEWORK

3.1. Nature and regulation of the sector

3.1.1. Schedule 1, item 2 of the FIC Act was amended and took effect from Monday,19 December 2022 and now includes trust and company service providers (TCSPs) as accountable institution (AIs). Accountants who perform any of the TCSP activities listed under item 2 of the FIC Act are regarded as accountable institutions. This report focuses on the money laundering and terrorist financing risks of institutions and individuals performing accounting services and does not include independent auditors, internal auditors or tax advisors that are not performing accounting functions.

3.1.2. The FIC has issued guidance to the sector in the form of public compliance communication (PCC) 6A to clarify the scope of TCSPs. PCC 6A states that:

“A person who performs the activities of a TCSP, regardless of the professional accreditation they hold, is an accountable institution. Any person that carries on any one or more than one of the listed activities under amended item 2 of Schedule 1 is

an accountable institution and is collectively referred to as a trust and company service provider (TCSP). Given that the TCSP definition is based on the activity that is performed by a person, it means that different professions are included in this category.

A TCSP in terms of item 2 of Schedule 1 to the FIC Act, is dependent on the activity performed. As such, a person that performs the business of a TCSP, regardless of the professional accreditation they hold, is an accountable institution and must register as a TCSP with the FIC. In practice, this means that financial institutions, legal professionals and accountants, among others, can meet the definition of a TCSP."

3.1.3. The FIC's approach is to include AIs in the FIC Act based on those activities that pose the highest ML and TF risks and not merely based on the profession.

3.1.4. Schedule 1, item 2 of the FIC Act defines a TCSP as follows:

(a) A person who carries on the business of preparing for or carrying out, transactions for a client, where-

(i) the client is assisted in the planning or execution of-

(aa) the organisation of contributions necessary for the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008 (Act 71 of 2008);

(bb) the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008; or

(cc) the operation or management of a close corporation, as defined in the Close Corporations Act, 1984 (Act 69 of 1984.)

(b) A person who carries on the business of-

(i) acting for a client as a nominee as defined in the Companies Act, 2008 (Act 71 of 2008); or

(ii) arranging for another person to act for a client such as a nominee.

(c) A person who carries on the business of creating a trust arrangement for a client.

(d) A person who carries on the business of preparing for or carrying out transactions (including as a trustee) related to the investment, safe keeping, control or administering of trust property within the meaning of the Trust Property Control Act, 1998 (Act 57 of 1988).

3.1.5. PCC 6A further clarifies that TCSPs do not include the following:

- Activities that relate solely to the recording, or capturing of company data or information, including book-keeping functions
- The administrative submissions of information or data for legislative purposes, such as the filing of tax returns
- Activities that do not amount to decision-making within the client's business activities
- Activities that do not steer, impact or influence the client's business operations.

3.1.6 Although these activities do not constitute the business of a TCSP and are not subject to FIC Act obligations, it must always be noted that the reporting of suspicious and unusual transactions under section 29 of the FIC Act applies to all businesses.

3.1.7 The fulfilling of a statutory function, specifically the liquidation of an entity or the functions of business rescue, is not considered to meet the definition of operations or management of a client. However, if the client undergoing such a statutory application is themselves an accountable institution in terms of Schedule 1 to the FIC Act, this client would remain an accountable institution, and the appointed liquidator or business rescue practitioner would be required to make sure their client applies the full provisions of the FIC Act in relation to their (the client's) business activities.

3.1.8 The accountancy profession in South Africa is not supervised by a statutory regulator. Accountants may choose to belong to any local or international professional association. Accountants who also perform the function of an auditor are required to register with the Independent Regulatory Board for Auditors (IRBA) as an auditor. It

is also possible that some accountants may act as a financial services provider by providing advisory and/or intermediary services in respect of a financial product. In such instances, they are required to register under the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002).

4. THE INTERNATIONAL MONEY LAUNDERING (ML) RISKS, AND TERRORIST FINANCING (TF) RISKS ASSOCIATED WITH ACCOUNTANTS

4.1 The accountancy profession is internationally recognised as potentially vulnerable to being abused by criminals to launder their proceeds of crimes. There are several key risks common to accountants of which they need to be aware, as follows:[2]

- the use of accountants to legitimise funds;
- organised crime groups trying to infiltrate legitimate accountancy practices and service provider or corrupt their employees;
- the use of client accounts to legitimise fund movements;
- criminals taking advantage of weak or inadequate risk assessments, policies, controls or procedures.

4.2 Professional accountants in public practice provide a wide range of services such as:

- Audit and assurance services (including reporting accountant work in initial public offerings;
- Bookkeeping and the preparation of annual and periodic accounts;
- Tax compliance work;
- Tax advice;
- Trust and company services;
- Internal audit (as a professional service), and advice on internal control and risk management;
- Regulatory and compliance services, including outsourced regulatory examinations and remediation services;

[2] See the United Kingdom HMRC Guidance on Understanding risks and taking action for accountancy service providers, Published 17 February 2021, at https://www.gov.uk/government/organisations/hm-revenue-customs.

- Company liquidation/insolvency/receiver-managers/bankruptcy related services;
- Advice on the structuring of transactions;
- Due diligence in relation to mergers and acquisitions;
- Succession advice;
- Advice on investments and custody of client money;
- Forensic accounting.

4.3 Some of the functions performed by accountants below make them potentially vulnerable to money laundering abuse:

4.4 Standard accountancy services – Low risk**:**

4.4.1 The following standard accountancy services may be considered low risk:

- Financial and tax advice – criminals may pose as individuals seeking financial or tax advice to place assets out of reach to avoid future liabilities.
- Gaining introductions to financial institutions – criminals may use accountants as introducers or intermediaries. This can occur both ways as criminals may use financial institutions to gain introductions to accountants as well.

4.5 Medium to High risk:

4.5.1 The following accountancy services may be considered high risk, depending on the facts and complexity of the legal person or arrangement (trust) structures and transactions involved :

- Company and trust formation – criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements e.g. trusts.
- Buying or selling of property – criminals may use property transfers to serve as either the cover for transfers of illegal funds (layering stage) or the final investment of these proceeds after it had passed through the laundering process (integration stage).
- Performing financial transactions – criminals may use accountants to carry out or facilitate various financial operations on their behalf (e.g. cash deposits or

withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers etc.).

- Maintenance of incomplete records by clients as revealed during the accounting or bookkeeping services provided by accountants can be an area of higher risk. In addition, the preparation, review and auditing of financial statements may be susceptible to misuse by criminals where there is a lack of professional body oversight or required use of accounting and auditing standards.

4.5.2 All accountants should be aware of risks areas such as criminals infiltrating or influencing accountants to conceal the origins of funds and the use of accountants to provide a sense of legitimacy to illegal transactions or activities.

4.5.3. South Africa has included TCSPs as accountable institutions as the services relating to the formation and management of companies and trusts are considered a particular area of vulnerability. Accountants who provide such services will therefore be regarded as accountable institutions under the FIC Act.

4.5.4 The FIC adheres to the FATF guidance on accountants which does not apply to professional accountants in business including professional accountants employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not-for-profit sector, regulatory bodies or professional bodies.

5. REPORTING BY ACCOUNTANTS UNDER THE FIC ACT

5.1 Accountants who do not fall within the definition of a TCSP are not regarded as accountable institutions in terms of the FIC Act and there is therefore no regulatory reports received from them (as accountants). During the financial year from 1 April 2022 to 31 March 2023, all trust and company service providers submitted 254 Cash Threshold Reports and 17 Suspicious and Unusual Transaction Reports

6. RISKS IN ASSESSMENT ALIGNED TO FIC GUIDANCE

6.1 The risk factors used in this sector risk assessment

6.1.1 The risk factors used in this sector risk assessment align with those used in the FIC's Guidance Note 7 which also includes a short reference to terrorist financing risk. Guidance Note 7 is available on www.fic.gov.za. Accountants must consider these factors when conducting their daily business.

6.2 Products and services risks

6.2.1 Certain products and services are regarded as posing a higher risk for money laundering purposes.

6.2.2 The products and services accountants provide that are internationally recognised as more likely to be abused by criminals in the money laundering process include:

- Company and trust formation – criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements e.g. trusts.

6.2.3 The method of payment for services provided by accountants could, in some instances, also be a channel for money laundering. The use of cash usually points to a higher risk for money laundering because it is more difficult to trace its origin.

6.2.4 Accountants that perform the role of a trustee or a director of a company, in particular in the capacity of independent trustees or directors, are required to obtain the

necessary information about the nature of the transactions of the trust or company, the natural persons or legal persons that are parties to transactions with the trust or company and ascertain whether the transactions make economic or commercial sense. They must also determine the origin of the funds received by the trust or company to make an informed decision about the ML and TF risks associated with such a transaction.

6.2.5 Although potentially a lower risk area, accountants that draw up financial statements should consider instances where there is a lack of original documentation as a potentially higher risk area.

6.2.6 Transactions that appear to be unrelated to the business of the client should be subject to additional scrutiny. In instances where the business of the client of the accountant is under financial strain, the client may resort to other sources of income and in such instances the accountants should, if necessary, obtain additional information on the transaction to verify its legitimacy.

6.3 Client risks

6.3.1 Listed as accountable institutions under the FIC Act, TCSPs are required to assess, identify, understand and then risk-rate the inherent money laundering and terrorist financing risks associated with their clients. Some clients, such as domestic politically exposed persons (DPEPs), foreign politically exposed persons (FPEPs), prominent influential persons (PIPs), complex legal structures or foreigners, potentially pose a higher risk for money laundering, depending on the identified circumstances. The establishment of complex local or international structures involving legal persons (companies) and legal arrangements such as trusts and partnerships – including where such structures are named as beneficiaries for a trust – could possibly be aimed at concealing the ultimate beneficial owners of such legal persons and arrangements. Enhanced due diligence should be considered in such instances.

6.3.2 Although accountants are not expected to have an in-depth knowledge of the business of all their clients, a basic understanding of such business activities will place the accountant in a better position to identify suspicious activities.

6.3.3 Where clients are hesitant to allow the accountant access to its business premises or its employees, it may make it difficult for the accountant to verify the financial information provided by the client. Such clients should be treated as potentially high risk.

6.3.4 When dealing with their clients, accountants should be aware of*, inter alia*, the following possible scenarios pertaining to the nature and behaviour of the clients that could point to possible money laundering:

- Clients trying to conceal their identities;
- Transactions inconsistent with their stated income or occupation;
- Clients use an unusual source of funds to transact;
- Transactions do not have a legitimate or economic reasons;
- Clients cease their business relationships upon a request for customer due diligence (CDD) information;
- Clients requesting funds to be paid into or from a third-party account that have no obvious link to the client;
- Clients that are difficult to reach or hesitant to provide customer due diligence information and information on their business activities.

6.4 Transaction risks

6.4.1 International best practice and literature relating to the ML/TF risks of the accountancy profession indicate that criminals can potentially use accountants to transact on their behalf thereby creating an impression of legitimacy to transactions involving the proceeds of crime. Monitoring the nature and purpose of these transactions, their monetary worth and the means of payments involved, will contribute to understanding and monitoring the money laundering risks associated with such transactions.

6.4.2 Examples of transactions that are potentially high risk for money laundering include the use of cash or crypto currencies, the reversing of transactions with a request to repay funds already paid and transactions that do not make economic sense. Accountants should be aware of the potential money laundering risks associated with such transactions and take the necessary steps to mitigate such risks.

6.4.3 In some instances, transactions may be split unnecessarily across different providers of accounting services to prevent anyone involved in the transactions getting a full picture and raise suspicion. Accountants must attempt to obtain additional information if it is suspected that a transaction forms part of a larger range of transactions.

6.4.4 The unnecessary use of loans by the client of an accountant could be done to conceal the origin of illegal funds, where the accountant notes that such loans are being repaid earlier than originally agreed on.

6.4.5 In addition to considering whether a transaction makes economic and business sense and whether the prices of assets obtained or disposed of are market related, an accountant must consider the use of cash by their clients in the buying, selling, and renting of properties or other assets.

6.4.6 In South Africa, cash is still used extensively. Accountants should be aware of instances where cash is paid into their accounts or the accounts of their clients, which could point to illegitimate funds or could be used to conceal the origin of the funds.

6.5 Risks relating to delivery channels

6.5.1 Accountants must be aware of the delivery channels they use to attract and deal with clients. Delivery channels that may obscure or conceal the true identity of the client, or that result in clients not being on-boarded face-to-face, may increase the risk of the accountant being abused by criminals to launder the proceeds of crime. Where an intermediary is used to on-board clients, an accountant must do proper due diligence on the intermediary and its business and must be familiar with the risk-mitigation processes and procedures the intermediary may have in place. It is also advised that, in such instances, the correctness of client information obtained by such intermediary be verified, albeit on a sample basis.

6.5.2 Various forms of technology are used to advertise services and conduct business. Where social media platforms and third-party service providers are used to share information on products or services or to on-board clients, an accountant must ensure

that such clients are properly identified and verified and that all the relevant information pertaining to the risks posed by such clients are obtained.

6.6 Geographic risk

6.6.1 Some foreign jurisdictions pose a higher risk for money laundering. It is important that accountancy practitioners be aware of the risks posed by clients from these jurisdictions and that they have the necessary risk mitigation processes in place. This risk is exacerbated by the fact that transactions can take place electronically across regions and national jurisdictions and that such transactions often require the services of accountants.

6.6.2 The geographic location and services provided by accountants are also important factors for determining ultimate money laundering risks. International and domestic experience has indicated that criminals are attracted to high-value assets, particularly high-end immovable property in exclusive or seaboard areas in South Africa, and therefore accountants need to be vigilant when conducting business in areas where such assets are acquired.

6.6.3 Accountants must be aware of the potential higher risks posed by clients (including their directors or trustees, shareholders and branches or subsidiaries), transactions or counterparties involving types of countries that are:

- Subject to a travel ban;
- Regarded by FATF as a high ML risk;
- Regarded as high-secrecy jurisdictions;
- Regarded as “tax havens”;
- Known to have high levels of organised crime, corruption or from which terrorist organisations are known to operate;
- Subject to United Nations sanctions;
- Generally known to provide funding or support to terrorist organisations or that host such organisations, including their neighbouring countries;
- Regarded as having weak governance systems, law enforcement and regulatory regimes, including countries regarded by FATF as having weak AML and CFT regimes.

6.7 Terrorist financing and proliferation financing risks

6.7.1 Where accountants provide services to non-profit and non-governmental organisations, they should ensure that the funds used are in accordance with the stated objectives of these organisations.

6.7.2 Accountants should also be aware of the appropriate compliance obligations referred to in sections 26A and 28A of the FIC Act which relate to the screening of clients to ensure that clients are not included in United Nations sanctions lists.

6.7.3 Accountants must know how to access the referenced targeted financial sanctions list and determine whether they are conducting business with individuals and institutions on such lists.

6.7.4 Requests for accounting services from offshore clients or local clients with offshore operations may possibly carry a higher risk for terrorist financing and financing the proliferation of weapons of mass destruction, depending on the nature of the client's business and their geographic location. Accountants must be aware of such higher risk areas and must take the necessary steps to mitigate and manage these risks.

6.7.5 Clients that are involved in the manufacturing or distribution of any product that may be used in the proliferation of weapons of mass destruction or that are exporting to countries regarded as high risk for such activities, including countries that are geographically close to high-risk countries, should be considered for enhanced due diligence.

6.7.6 Where an accountant identifies payment from or to the client for travel arrangements to or from high-risk terrorist jurisdictions, enhanced due diligence must be applied.

6.7.7 Clients that are claiming to provide loans or finance to individuals and institutions – particularly in high-risk areas – need to be scrutinised to determine whether such "loans" are being repaid.

6.7.8 Clients that appear to have extremist political, religious or world views, may potentially carry a higher risk for terrorist financing and may have to be subjected to enhanced due diligence.

7 INDICATORS OF ML AND TF ACTIVITY FOR THE SECTOR

7.1 The following could be regarded as ML and TF threats, vulnerabilities and risks associated with accountants:

- The use of cash for payment of services;
- Anonymity of clients and transactions that are complex in nature;
- New payment technologies e.g. crypto currencies;
- Lack of ML and TF awareness of the accountants;
- Requests for trusts, shell companies and other legal arrangements with a potential to conceal the true identity of the ultimate beneficial owners of the clients;
- International payments received from clients, particularly directly or indirectly from high-risk jurisdictions;
- High-risk customers and jurisdictions such as clients linked to institutions or jurisdictions on any sanctions list;
- Domestic Politically Exposed Persons (DPEPs), Foreign Politically Exposed Persons (FPEPs), Politically Influential Persons (PIPs), and high-net-worth individuals which are internationally regarded as high-risk clients;
- Organised crime can use legal practitioners and accountants to conceal the proceeds of crime, obscure ultimate ownership through complex layers and legal entity structures, avoid paying tax, work around financial regulatory controls, create a veneer of legitimacy to criminal activity, create distance between criminal entities and their illicit income or wealth, avoid detection and confiscation of assets, and hinder law enforcement investigations;
- Clients who offer to pay extraordinary fees for services that would not warrant such fees;
- Payments from non-associated or unknown third parties and payments for fees in cash where this practice is not typical;
- Where accountants, including those acting as financial intermediaries, physically handle the receipt and transmission of funds through accounts they control. They may be requested to transfer assets between parties in an

unusually short period, thereby hindering the know-your-client process and potentially contribute to concealing the beneficial ownership of the client or other parties to the transactions(s) from competent authorities;

- Funds are received from or sent to a foreign country when there is no apparent connection between the country and the client;
- The client is using multiple bank accounts or foreign accounts without good reason;
- Possible involvement of DPEPs, FPEPs and PIPs in instances where the entity, structure or relationships of the client make it difficult to identify its beneficial owner or controlling interests e.g. the unexplained use of legal persons or legal arrangements;
- Instances where clients, for no apparent reasons, change the way in which transactions are concluded or change their instructions to the accountant on short notice or in a manner that does not make economic sense.

8 CONCLUSIONS

8.1. Based on the international experience, the risk factors described above and the range of services they offer, it is evident that accountants who are TCSPs are potentially at high risk of being exposed to the inherent risk of ML. They should therefore take all the necessary precautionary steps to reduce the risk of being exposed to abuse by criminals who want to launder the proceeds of crime through the sector.

8.2 The use of cash is evident and appears prevalent in the accountancy sector which increases the ML and TF risk profile of accountants.

8.3 Overall, the inherent risk of money laundering for the accountancy sector involved in TCSP activities in South Africa, based on national and international experience, is classified as a sector as inherently medium to high. Accountants that provide standard accountancy services are classified as low.

8.4 Accountants who provide services to non-profit organisations are at a higher inherent terrorist financing risk and those that provide standard accountancy services are regarded as low.

8.5 The provisions of the FIC Act are aimed at making it more difficult for criminals to launder the proceeds of criminal activities through accountable institutions. It is envisaged that the inclusion of accountants that are providing the services of a TCSP as accountable institutions would be a deterrent for criminals wishing to use this avenue to launder illicit funds.

9 CONSULTATION

9.1 Commentators are invited to comment on the sector risk assessment by submitting written comments via the online comments submission link only. Any questions or requests relating to this sector risk assessment may only be sent to the FIC at consult@fic.gov.za. Submissions will be received until close of business on Friday, 17 November 2023.

9.2 The FIC intends to conclude the consultation on this sector risk assessment by publishing a final version as soon as possible, but no later than Thursday, 14 December 2023.

Issued by:
The Financial Intelligence Centre
6 November 2023