

FOR CONSULTATION

**Risk and compliance return in terms of section 43A of  
the Financial Intelligence Centre Act, 2001 (Act 38 of  
2001) (FIC Act).**

DETAILS OF INSTITUTION	
Full registered or legal name	
Business address	
Contact number	
E-mail address	
Institution's representative(s)	
ORG ID number	
Sector	
Institution type	
Location	

ABOUT THE INSTITUTION			
Structure of the institution. Please mark with a "X"			
<input type="checkbox"/>	Public company	<input type="checkbox"/>	Private company
<input type="checkbox"/>	Sole proprietor	<input type="checkbox"/>	Partnership
<input type="checkbox"/>	Close corporation	<input type="checkbox"/>	Other specify

List the institution's products or services	
Annual turnover for the last financial year	
Does any senior manager or beneficial owner of the institution have criminal charges?	
Number of employees	

DECLARATION

**Click or tap here to enter text.** declare that the information contained in this risk and compliance return questionnaire is, to the best of my knowledge, comprehensive and correct, and that it will promptly file any needed supplemental information.

I, **Click or tap here to enter text.** Of the abovementioned institution do hereby certify that this declaration was read and understood, that the information provided in this risk and compliance return is accurate and complete, and that I am duly authorised to execute this declaration on behalf of the abovementioned institution.

---

**SIGNATURE**

---

**DATE**

Please select the correct answers from the drop-down options.

**PART 1 – GENERAL RISK QUESTIONS**

Questions		July 2023 – March 2024	April 2024 – March 2025	April 2025 – March 2026
1.1.	What percentage of your clients are natural persons?			
1.2.	What percentage of your natural person clients are foreign nationals?			
1.3.	What percentage of your clients are foreign legal persons?			
1.4.	What percentage of your clients are trusts?			
1.5.	Does your institution conduct business with any domestic politically exposed persons (PEPs) or their close family members or close associates?			
1.6.	What percentage of your clients have been identified as high-risk domestic PEPs?			
1.7.	What percentage of your clients have been identified as high-risk Domestic Prominent Influential Persons?			
1.8.	Does your institution conduct business with any foreign PEPs?			
1.9.	What percentage of your clients have been identified as foreign PEPs?			
1.10.	Does the institution onboard clients on a non-face-to-face basis (i.e. social media platforms, electronic platforms or agents?)			

1.11.	Does your institution accept cash in the conclusion of any transactions (not applicable to electronic funds transfers)?			
1.12.	Do you allow third parties to transact on behalf of your clients?			
1.13.	Has your institution refunded or reversed client monies paid into your accounts where a client had not provided KYC documents?			
1.14.	Does your institution conduct cross-border transactions?			
1.15.	Does your institution screen employees against the TF list?			
1.16.	Do you "risk rate" your products and services for ML/TF/PF when introducing new products and services?			
1.17.	Is your institution situated within 100km of an international border?			
1.18.	Does your institution conduct business with clients from countries regarded as high-risk for ML/TF/PF purposes?			
1.19.	Does your institution conduct business with clients from countries regarded as tax havens or high-secrecy jurisdictions?			
1.20.	Does your institution conduct business with clients from countries on the Financial Action Task Force blacklist?			
1.21.	Does your institution screen potential clients against the TFS list before onboarding?			
1.22.	Does your institution screen its clients against the TFS list when the list is updated?			
1.23.	Are you aware of the appropriate compliance obligations that arise when conducting business with individuals and institutions on such lists?			
1.24.	Does your institution have a risk management and compliance programme (RMCP) implemented?			

1.25.	Does your institution have branches and/or subsidiaries?			
1.26.	Does your institution have a compliance function?			
1.27.	Does your institution provide ongoing training to its employees to enable them to comply with the FIC Act and the RMCP?			
	Identification of clients and other persons.			
1.28.	Does your institution have processes and procedures in place for the identification and verification of clients?			
	Politically exposed persons, family members and known close associates			
	Does your institution have processes and procedures in place to establish whether a prospective client or beneficial owner of the prospective client in a business relationship is a:			
1.29.	Foreign politically exposed person?			
1.30.	Family member or known close associate of the foreign politically exposed person?			
1.31.	Domestic politically exposed person			
1.32.	Family member or known close associate of the domestic politically exposed person			
	Understanding and obtaining information on business relationships			
	Does your institution establish the:			
1.33.	Nature of the business relationship?			
1.34.	Intended purpose of the business relationship?			
1.35.	Source of funds?			
	Additional due diligence measures relating to legal persons, trusts, and partnerships			
	When the client is a legal or natural person who is acting on behalf of a partnership, trust, or similar arrangements between natural persons, does the institution establish the:			

1.36.	Ownership and control structure of the client?			
1.37.	Does your institution establish the identity of the ultimate beneficial owner/s of the client?			
1.38.	Does your institution establish the identity of the natural person who exercises effective control of the legal person client?			
1.39.	Does your institution establish the identity of each founder and trustee and beneficiary of the trust (where the client is a trust)?			
1.40.	Does your institution establish the identity of the founder/trustee/beneficiary of the trust if the founder/trustee/beneficiary is a legal person? (where the client is a trust)			
	Ongoing due diligence			
	Does your institution monitor transactions undertaken throughout the course of the business relationship, including:			
1.41.	Ascertaining the source of funds			
1.42.	Background and purpose of complex, unusual large transactions			
1.43.	Unusual patterns of transactions which have no apparent business or lawful purpose			
1.44.	Does your institution keep the customer identification and verification documents up to date?			
1.45.	Does your institution take additional steps when it has doubts about the veracity or adequacy of previously obtained information?			
	Inability to conduct customer due diligence			
1.46.	Does your institution file regulatory reports with the FIC under section 29 of the FIC Act if unable to conduct customer due diligence?			

1.47.	Does your institution keep records on clients?			
1.48.	Does your institution keep records of client information?			
1.49.	Does your institution keep records of transactions?			
1.50.	Does your institution keep client records for five years after the termination of a business relationship?			
1.51.	Does your institution use a third party to keep client records?			
	If yes to the previous question, does your institution have sufficient information about the third party and does the institution:			
1.52.	Have free and unencumbered access to the relevant records?			
1.53.	Are the records kept by the third party readily accessible to the FIC and/or the relevant supervisory body when required?			
1.54.	Are the records capable of being reproduced in a legible format?			
1.55.	Have the full name and contact particulars of the individual who exercises control over access to those records?			
1.56.	Have the address where the records are kept?			
	<b>Regulatory Reporting</b>			
1.57.	Did your institution file section 28 reports (cash threshold reports) for the reporting period?			
1.58.	Has your institution filed reports under section 28A i.e., terrorist property reports, during the reporting year?			
1.59.	Does your institution have a process in place for the identification and reporting of suspicious and unusual transactions S29 reporting?			

1.60.	Is your institution's staff aware that they may not disclose information about the contents of section 29 reports?			
1.61.	Was your institution served with any subpoenas in terms of section 205 Criminal Procedures Act, 1977 (Act 51 of 1977), received any enquiries or requests for information from the FIC, investigative authorities or other regulatory bodies in respect of any transaction concluded with a client?			
1.62.	Have any clients of your institution enquired as to whether your institution had reported them to the FIC?			
1.63.	Does your institution have processes and procedures in place to deal with a section 32 request from the FIC?			

## PART 2 – PROLIFERATION FINANCING

	Questions	July 2023 – March 2024	April 2024 – March 2025	April 2025 – March 2026
2.1.	Do you have any dealings/interactions with clients that provide products and services to countries that are listed considered high risk for PF purposes (Iran and The Democratic People's Republic of Korea)			
2.2.	Do you have any dealings/interactions with countries listed on the FATF Blacklist?			
2.3.	Do you produce or deal in products that may be used in the proliferation of weapons of mass destruction?			
2.4.	Do you assess PF risks related to dual-use goods?			
2.5.	Do you screen for PF red flags from FATF Guidance 2024?			
2.6.	Do you have PF risk factors unique to identify possible instances of PF when dealing with clients?			

2.7.	Do you have clients that are nationals of countries that are FATF black-listed? Which percentage?			
2.8.	Do you have clients that process funds to or from countries that are on the FATF blacklist?			
2.9.	Do you follow a process to screen all existing client information against updates to the TFS list without delay?			
2.10.	Do you have clients that deal with controlled good or dual use goods? Refer to PCC 44A on targeted financial sanctions.			
2.11.	Do you follow a process to freeze without delay funds that are linked to a designated person?			
2.12.	Do you follow a process to report without delay funds or business relations that are linked to a designated person?			
2.13.	Do you identify beneficial owners of clients that are foreign legal companies or arrangements?			
2.14.	Do you provide training to staff on aspects of proliferation financing?			

### PART 3 – TERRORIST FINANCING

No.	Questions	July 2023 – March 2024	April 2024 – March 2025	April 2025 – March 2026
3.1	Does your institution operate in any areas that are considered a high risk from a TF perspective? Consider media reports and crime statistics			
3.2	Do you have customers that are citizens from countries that are subject to UNSC sanctions measures?			
3.3	Do you conclude transactions to or from the geographic locations that pose a heightened risk of terrorist financing?			

3.4	Do you transact with CASPs or accept crypto assets as payment from countries that are pose a high risk for terrorist financing?			
3.5	Do you have clients that are complex legal structures, legal persons or trusts that are from countries that are highlighted in the 2024 TF NRA?			
3.6	Do you accept payments of prepaid cards, Money Value Transfer Services (mobile money) or Alternative remittance services?			
3.7	Do you accept third parties to collect cash on behalf of money remitters?			
3.8	Do you send funds to countries in Africa that are known for terrorist activity?			
3.9	Do you conduct transactions with clients that facilitate transfers to high-risk countries from a terrorist financing perspective?			
3.10	Do you conduct transactions with hawala and remittance networks??			
3.11	Do you facilitate travel to and from conflict areas?			
3.12.	Do you conduct transactions in crypto assets or trade in commodities (oil, diamonds, or gold?)			
3.13	Do you establish business relationships with clients using passports, asylum seeker/ refugee permits as proof of identity?			
3.14	Do you conduct transactions of gold coins and / or foreign currency?			

3.15	Does your institution conduct business with dealers of precious metals or stones (DPMS) that are in proximity (less than 100 kms) to conflict areas?			
3.16	Do you conduct transactions with non-profit organisations and/or non-governmental institutions?			
3.17	Do you conduct business with unregistered or voluntary NPOs?			
3.18	Do you conduct business with charities and organisations involved in health, faith based, humanitarian and educational work operating in terror/ conflict areas?			
3.19	If answered yes above, do you ensure that the use of the funds and / or properties involved are used in accordance with the stated objectives of these organisations?			
3.20	Have you submitted an STR/SAR relating to TF/PF in the last year?			
3.21	Does your institution conduct business with clients in the arms/ national defence industry?			
3.22	Does your institution conclude transactions with customers from countries that are involved in armed conflict or terrorist activity?			
3.23	Does your institution conduct business with customers that have a significant social media presence, and allege to be raising funds for charitable organisations in conflict areas?			
3.24	Do you monitor TF crowdfunding typologies?			
3.25	Do you track clients linked to the Islamic State of Iraq and the Levent (EI/ISIL) returnees?			
3.26	Where you suspect that a potential client is a sanctioned			

	<p>person or entity or is linked to a sanctioned person or entity?</p> <p>Do you have processes to further investigate the validity of this suspicion (e.g. do you scrutinise their information against the TFS list, do you conduct an adverse media search)?</p>			
3.27	Do you have a process in place to report without delay to the FIC where a designated person or entity tries to transact with you?			
3.28.	Do you follow a process to scrutinize client information against the TFS lists without delay from date of updates to the TFS list?			
3.29.	Within which period do you screen you client data against the TFS list?			
3.30	Do you monitor developments on domestic terrorist activity?			
3.31	Do you screen your client information without delay against the section 23 POCDATARA court orders as published by the from time to time?			

#### PART 4 – LEGAL PRACTITIONERS

	Questions	July 2023 – March 2024	April 2024 – March 2025	April 2025 – March 2026
4.1	<p>1. Which category of legal practitioners do you belong to?</p> <p>4.1.1 S111- Legal Practitioners (Attorneys)</p> <p>4.1.2 S111- Legal Practitioners (Advocates with Trust Account)</p>			

	4.1.3 A commercial juristic entity as contemplated in the Legal Practice Act			
	<b>Products and Services</b>			
4.2	Do you provide any of the following services in your legal practice? a) Conveyancing: Assisting with the transfer of property, including drafting of documents, managing property transactions with overstated or understated values, or facilitating the transfer of properties to third parties.			
	b) Business in a Customer Account: Assisting with financial transactions where funds are placed in your client account, including situations where purchases or investments may not take place or where funds are transferred to a third-party account.			
	c) Formation and Management of Legal Entities: Creating and managing legal entities such as complex legal structures, or shell companies that could obscure the true ownership of assets.			
	<b>Cash Payments and Trust Accounts</b>			
4.3	Do you accept cash payments for services or payments into trust accounts?			
4.4	If yes, do you have procedures in place to assess and mitigate the risks associated with cash payments, particularly those that might indicate money laundering activity?			
	<b>Anonymity and Complex Transactions</b>			
4.5	Have you provided legal advice or services for clients that are complex in nature and where the client's identity (including BOs) is not clear?			

4.6	If yes, do you verify the legitimacy of these clients to prevent the potential misuse of your services for money laundering or terrorist financing?			
4.7	Have you provided legal advice or services for transactions that are complex in nature and the transaction's purpose is not clear?			
4.8.	If yes, do you verify the legitimacy of these clients and transactions to prevent the potential misuse of your services for money laundering or terrorist financing?			
New Payment Technologies				
4.9.	Do you accept payments through new technologies, such as crypto assets, for your legal services?			
4.10.	If yes, do you have measures to mitigate the risks associated with these payment methods, particularly in relation to money laundering or terrorist financing?			
International Payments				
4.11	Do you receive payments from clients located in foreign countries?			
4.12.	If yes, do you have measures to ensure that these payments are legitimate, especially when there is no apparent connection between the country and the client?			
Extraordinary Fees				
4.13.	Have you encountered situations where clients offer or pay extraordinary fees for services that would not typically warrant such high fees?			
4.14.	If yes, do you assess and address the risks associated with these unusual payment arrangements?			
Fictitious or questionable debts				
4.15.	Have you ever encountered instances where clients have requested your services to recover fictitious or questionable debts?			
4.16.	If yes, do you have measures in place to identify fictitious debt?			
Transactional reversal				

4.17.	Have you encountered an instance where your client requests reverse transactions with repayment of funds, or transactions that do not make economic sense?			
4.18.	If yes, do you evaluate whether a transaction makes economic and business sense?			
4.19.	Do you accept Third-Party Payments?			
4.20.	If yes, do you have controls in place to verify the source and legitimacy of these payments?			
	<b>Handling of Funds and Real Estate Transfers</b>			
4.21.	If you physically handle the receipt and transmission of funds through accounts you control, have you been requested to transfer real estate between parties in an unusually short period?			
4.22.	If yes, do you have controls in place to ensure that these transactions do not contribute to concealing the beneficial ownership of the client or other parties involved?			
	<b>Funds from or to Foreign Countries</b>			
4.23.	Have you received or sent funds to a foreign country when there is no apparent connection between the country and the client?			
4.24.	If yes, do you conduct due diligence measures to verify the legitimacy of these transactions?			
	<b>Multiple Bank Accounts</b>			
4.25.	Do any of your clients use multiple bank accounts or foreign accounts without an apparent legitimate reason?			
4.26.	How do you assess and manage the risks associated with such practices?			
	<b>Changes in Transaction Patterns</b>			
4.27.	Have you observed instances where clients change the way transactions are concluded or alter their instructions on short notice without apparent reason?			

4.28.	If yes, do you have measures in place to assess whether these changes make economic sense, and how do you manage the associated risks?			
Complex Legal Structures				
4.29.	Do you deal with clients who establish complex structures involving companies, trusts, or partnerships?			
4.30.	If yes, do you take steps to identify and verify the ultimate beneficial owners (UBOs) in such complex structures?			
Intermediaries and Third-Party Service Providers				
4.31.	Do you use third-party service providers or intermediaries to assist with client identification, verification, or onboarding?			
4.32.	If yes, do you conduct due diligence measures to assess the intermediary's business, including their risk mitigation processes and procedures?			
Indicators of Suspicious Client Behaviour				
4.33.	Have you encountered any of the following client behaviours that may indicate potential money laundering?			
	a) Clients attempting to conceal their identities.			
	b) Transactions inconsistent with the client's stated income or occupation.			
	c) The use of unusual sources of funds for transactions.			
	d) Transactions lacking a legitimate or economic reason.			
	e) Clients ceasing their business relationship upon a request for customer due diligence (CDD) information.			
Verifying Source of Funds				
4.34.	Do you inquire about the source of funds involved in legal matters, such as property transactions or trust establishment?			
Cross-Border Transactions				

4.35.	Do you engage in cross-border legal transactions?			
4.36.	If yes, do you assess and manage the risks related to these transactions, especially those linked to countries with higher ML/TF/PF risks?			
	<b>ML/TF Awareness</b>			
4.37.	Do you detect abuse of legal structures using global typology indicators?			
4.38.	Do you perform sanctions screening for cross-border fund flows?			