AGENT AID

# INFO SESSION

## LATEST ON RMCP REQUIREMENTS AS PER GUIDANCE NOTE 7A, SUBMISSION OF RMCP'S AND COMMON NON-COMPLIANCE ISSUES

# Table of Contents

# What should be included in your RMCP as per Guidance note 7A

Guidance note 7A was issued by the Financial Intelligence Center as a replacement to Guidance note 7. Guidance Note 7A covers all aspects of what should be covered in an Accountable Institution's Risk Management Compliance Programme (RMCP).

During an online webinar held on 7 March 2025, FIC confirmed that only 1 of the 5 chapters in Guidance Note 7A have been updated, and that the rest of the sections will be updated in future updates.

It is important to stay updated on what should be included in your firm's RMCP – you should upload all your updated / revised RMCP's in the same manner as will be described later in this document.

**VERY IMPORTANT:**

**Your RMCP is not meant to be a document that you draft once and leave to gather dust. Your RMCP is your blueprint on how you handle FIC matters within your business. Your Employees must be aware of their obligations, and your RMCP should be a realistic reflection of how you implement FIC Act obligations in your organization.**

We have divided the RMCP into 3 sections, to aid in a logical flow of your RMCP.

## 1. Administrative Section

### 1.1. The Front Page

The Front page of your Risk Management Compliance programme should keep to a specific format. The recommended format is as follows, and includes the following:

- **Your firm Logo**. The Logo must be clear, and contain both the Picture / Logo and the name of your firm.
- The words '**Risk Management Compliance Programme**'
- The **Registered and trading as name of the firm**, as well as the **registration number** of the firm.
- It is not compulsory, but it is recommended to also include the following:
    - The Date the RMCP was compiled in full, for example 'as compiled on 2 February 2023' or 'as Revised on 5 March 2023'.
    - The Authors of the RMCP, for example 'Compiled by John Smith', and should either be top management, or the FIC Compliance Officer.

Your first page is the first impression that the Financial Intelligence Centre will have of your firm – ensure it is presented in a professional manner.

### 1.2. The Index

The Index is a basic table of contents of what is contained in your RMCP. The index, just as with any other index, will help anyone looking at the RMCP to easily navigate the contents of your RMCP.

The Index must be completed AFTER you have completed the rest of the file, to ensure accurate page numbering.

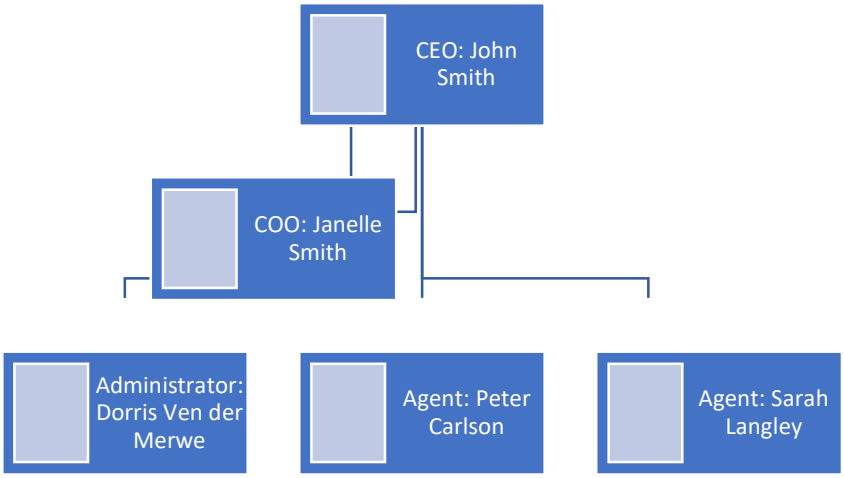
Your Index should contain:

- The **page numbers** of each item contained in the RMCP.
- The **Shortened names / headings** of each item contained in the RMCP.

## 1.3. Organogram of the Organisation

What is an organogram? An organogram is a diagram that displays the hierarchy of an organisation.

An organogram is only ever effective if it contains all members of the organisation. A simple visual representation of an organogram is as follows:




The following should be included in your organogram to ensure its effectiveness:

- A **Photo** of each member in the Organogram
- The **Full Title** of each member in the Organogram
- The **Full Names and Surnames** of each member in the Organogram

**All members within the organisation**. Leaving someone out of the Organogram defeats the purpose of the organogram. If the organisation is too big to contain on a one-pager organogram, it is recommended to do the organogram for top management, and key members within the firm, like administrative staff, and just attach a list for all members, categorized by hierarchy, that do not fit on the organogram or form part of the key staff members.

## 1.4. FIC Registration Confirmation

It is recommended that you keep proof of your FIC Registration in your RMCP. As it is compulsory to be registered with FIC because you are considered an accountable institution, instructions will be given below the following list on how to register on the FIC website, if you are not already.

The following are considered proof of registration with FIC:

- The Initial email received from FIC Confirming your organisation registration.

- A screenshot of your organisation details when you have logged into the FIC Website.

How to Register on FIC Website:

- Visit the following URL: https://goweb.fic.gov.za/goAMLWeb_PRD/WebRegistration/NewEntityCR
- Follow the instructions and provide the needed info.
- You will receive an email confirming your registration, or a request for further documentation / information, once you have submitted the form.

Why do we need to put FIC registration confirmation in our files, if the FIC already has these records? We want any stakeholder who sees the RMCP to know we are appropriately registered with the FIC, like employees and staff members.

## 1.5. Letter of Acceptance of RMCP by Top Management

**NB: This Obligation has changed with Guidance note 7A – thus if you have an RMCP already in place, please make sure to update this section**

Your RMCP must be signed off by your organization's top management. Top Management is anyone who:

- Holds at least 5% equity in your business
- Directors
- Top-level management / executive management

The Financial Intelligence centre requires this as proof that they are aware, and approve of the contents within the RMCP.

The following are important aspects to consider and include in the letter:

- All Directors of the firm as listed on the CIPC registration documents must review the RMCP and sign this acceptance letter.
- All top management not listed on the CIPC registration documents must review and sign this acceptance letter. This means, for example, the COO, the Office Manager, the Financial Manager. This will be unique to each organisation, so only have it signed by persons you deem to be part of top management.
- This letter must be dated and must be re-signed every time the RMCP is re-evaluated or changed.
- **The Letter must state that each member who have signed:**
    - **Understand that they are responsible to ensure compliance with the FIC Act.**
    - **That they guarantee the RMCP as presented is Adequate, Suitable and Effective.**
    - **That they have applied their minds when considering the approval of the RMCP as presented by the Compliance Officer.**

## 1.6. FIC Officer / MRLO Officer Appointment Letters

**What is a FIC Compliance Officer?**

A FIC Compliance Officer is responsible for the drafting of the RMCP, reporting obligations of a firm as the need arises, and implementation of the RMCP across the organisational structure.

The default FIC Compliance officer would have been the person who registered the firm on the FIC's website. This can be amended with the FIC, if the need arises.

**What is an MRLO?**

Money Laundering Reporting Officer(s) can be appointed in a firm, if the need arises for a firm to have more than one person for reporting obligations. The MRLO is not compulsory, and only applicable if the firm has a need for more than one reporting officer. The FIC Officer is the default reporting officer.

The reason an MRLO exists, is because the FIC does not allow for password sharing within an organisation. The MRLO will only be responsible for making reports to the FIC when the need arises, and do not share any other of the responsivities of the FIC Compliance Officer.

The FIC Officer must be someone with adequate seniority to understand the inner workings of the firm in great detail. They must have the ability to access all parts and systems of the firm which give rise to FIC Requirements. This means that, the receptionist is most likely not the best candidate for the FIC Officer, but the Financial Manager is a good option.

It is not recommended that the Directors of the firm is the FIC Officer, unless there is no good alternative. The Directors might be ultimately responsible to ensure compliance with the FIC Act, but they often are not part of the day-to-day dealings within the organisation, and therefore may not be able to effectively evaluate risks. This is not applicable in sole proprietorships / small businesses where the Owners / Directors are the only employees of the firm.

Your RMCP must contain the appointment letters of your FIC Compliance Officer, and where applicable, any other MRLO's.

## 1.7. Decision-making order on Risk Matters

**This Section is where the chain-of-command must be explained for when a risk matter is raised.**

How is this different from the company organogram? The Organogram is focussed on the official structure of the company, focussing on official titles and positions held within a firm. The decision-making order in this context focuses specifically on the decision-making order for risk and FICA-related scenarios.

For Example, let us say an agent within the firm is questioning the veracity of previously obtained information. What channels are appropriate for them to follow to get a clear answer on whether they may do business with the client or not?

It could be common practice within your firm that they start with the transaction coordinator. If the transaction coordinator does not have the answer, they must refer it to the office manager. If the office manager does not know, it must be referred to the FIC Officer, and ultimately to the Principal.

This will look different for each firm. You can do this part in a flow-chart form or type it out.

It is important to mention the titles and full names of all parties involved in this chain of command. It is recommended to also include the following in this section:

- The Date Compiled
- The Company letterhead
- Contact details for all within the chain-of-command.

The reason this is separated from the organogram, is because the official hierarchy of an organisation is not always the same as the chain-of-command in FIC decision-making.

If you are a Sole Proprietorship or the only employee within the company, this point may be left out, as it does not apply to you.

## 1.8. Risk Defined, Risk rating Methodology, and Risk Analysis

The FIC expects of all accountable institutions to:

- Define risk,
- explain their risk rating methodology,
- and complete a risk analysis on their business, products and services, and clients.

The risk definition and risk rating methodology for most real estate entities will be largely similar, and therefore you can work off of FIC's recommended risk indicators for guidance, and use their risk definition.

**Risk definition and risk-rating methodology:**

We will define risk in the same way as the Financial Intelligence Centre does (as extracted from Guidance Note 7 of the FIC Act):

- According to international best practice risk rating methodology, risk refers to the likelihood and impact of uncertain events on set objectives. The impact can be either a positive or negative deviation from what is expected. This uncertainty is a function of three factors: threat, vulnerability, and consequence.
- The context of the above is important. For example, "threat" or "consequence" to whom or what. On the other hand, vulnerability could arise from external and internal factors and may be either controllable or uncontrollable.
- A threat is a person or group of people, object, or activity with the potential to cause harm. In the context of money laundering and terrorist financing this includes criminals, terrorist groups and their facilitators, their funds, as well as the past, present, and future money laundering or terrorist financing activities.
- The concept of vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. Identifying vulnerabilities, as distinct from threats, means focusing on, for example, the factors that represent

weaknesses or features that may be exploited in a given system, institution, product, service etc.
- Consequences refer to the impact of a threat or the exploitation of a vulnerability if this impact is to materialise.

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

**What are inherent and residual risks?**

- Inherent risk is the risk of an event or circumstance that exists before controls or mitigation measures are applied by the accountable institution.
- Residual risk is the level of risk that remains after controls and mitigation measures were implemented by the accountable institution.

**What are money laundering and terrorist financing (ML/TF) risks?**

- The concept of ML/TF risks, as the term implies, relate to threats and vulnerabilities that may promote the laundering of proceeds of unlawful activities or the financing of terrorism, on the one hand, or may jeopardise the detection, investigation or prosecution of these activities or the possibility of the forfeiture of proceeds of unlawful activities, on the other.
- On a national level these are threats and vulnerabilities which put at risk the integrity of South Africa's financial system and negatively impacts the administration of criminal justice which affects the safety and security of South Africans as well as that of people outside of South Africa.
- In relation to accountable institutions, ML/TF risks are threats and vulnerabilities which put the accountable institution at risk of being abused in order to facilitate ML/TF activities. These relate to the potential that clients, by using the accountable institution's products and services, can exploit the accountable institution to promote money laundering or terrorist financing activities. The nature of these risks relates to a number of aspects, including the features of the intended target market of clients who are likely to use an accountable institution's range of products and services, the geographic locations of an accountable institution's operations and of its clients, the delivery channels through which persons become clients of an accountable institution or through which clients access its products and services, the features of a particular product or service, etc.
- In order to have a robust ML/TF risk management system, accountable institutions must be able to demonstrate how they contextualise the concepts of "ML/TF risk" within their particular businesses as having an impact on their operational, line management and strategic objectives.
- Controls should be purposefully built and/or adapted to address ML/TF risks. Accountable institutions may make use of the controls which are already in place.

**Risk Appetite**

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

**Business-level risk**

The FIC expects of all accountable institutions to do a risk analysis on their Business. What is a risk analysis? A risk analysis is a snapshot of all risks your business currently faces. Your Risk analysis must include the following:

- Geographic Risk – Risks associated with your business's physical environment. This risk includes risks on the neighbourhood, city, province and country level. For example – all firms operating in South Africa has a risk for being misused for Money Laundering / Terrorist Funding activities, because our country is still present on the Grey List of the Financial Action Task Force (FATF).
- Staff Risk – the control you exercise over your employees can lead to higher risk for ML / TF activities. The more control you have, the lower the risk.
- Accounting / Bank Account Administration risk – depending on how many people have access to the business bank accounts and accounting systems, your firm could have a higher risk for ML/ TF risks. For example, delegation of tasks in accounting administration leads to a lower risk for ML/TF activities, because more than one person checks that transactions are correct and as intended. Your auditing process must also be referenced.
- Business Owner Expertise: The level of knowledge of business within your industry, can lead to your firm being at higher or lower risk for ML/TF activity – The more knowledgeable the business owner is in the industry they work in, and the better their reputation, the less risk.

For each risk addressed, a risk level must be allocated. You need to analyse the risk, and give it a rating out of Low Risk, Neutral Risk, or High Risk, and then give an overall score for Business-level risks.

Here is an example:

| Risk Indicators | Description / reasoning | Risk Rating |
|---|---|---|
| **Geographic Area** | • Our business operates in a high-income area.<br>• Our regional SAPS have functional service.<br>• We have active neighbourhood watch and security companies operating in the area.<br>• Most of the homeowners in our area are retired.<br>• Our business operates only in South Africa, and South Africa has high crime rates, especially that of a financial nature. | **Low** – The only factor that could increase the risk of Money laundering, Terrorist Financing and Proliferation financing in this context, is the fact that we operate in South Africa, but comparatively to other areas, the areas we operate in is lower risk. |

**Products and Services Risks**

Each Real Estate Agency has its own list of products and services they offer. Each product and service must be separately analysed for risk, and given a risk rating, depending on its likelihood to be used for ML/TF activities.

The following is a typical list of products and services within a real estate firm:

- Credit-worthiness Checks of clients
- Inspections
- Maintenance
- Rental monies management
- Utility account management
- Facilitation of Lease Agreements
- Facilitation of Sale Agreements
- Marketing and listing of properties for rent / sale
- Assisting with Municipal Applications
- Transaction coordination

You can use whatever established tool for analysis you prefer to complete a risk analysis and rating on each product / service, but the most common tool you can use, is a SWOT analysis.

Here is an Example:

<table>
<tr><td>Product:</td><td colspan="4">Credit-worthiness checks of clients</td></tr>
<tr><td rowspan="2">SWOT Analysis</td><td colspan="2">STRENGHTS<br>• Ensures that clients can afford lease payments / mortgage payments associated with lease agreements / offers.<br>• Mitigates ML/TF/PF activities because we can determine source of funds during this process.</td><td colspan="2">WEAKNESSES<br>• We rely on external systems and bureaus for the results of these credit worthiness checks, and thus we cannot control if the results are accurate or not.</td></tr>
<tr><td colspan="2">OPPORTUNITIES<br>• We can offer credit-worthiness services to other business to generate alternative income, because we are already subscribed to credit bureau services.</td><td colspan="2">THREATS<br>• Information provided for credit checks can be fabricated, and hardened criminals can fabricate years of details in order to pass a credit check without raising suspicion.</td></tr>
<tr><td>Discussion of Weaknesses:</td><td>Weakness:</td><td colspan="3">External Systems – no guarantee of accuracy</td></tr>
<tr><td></td><td>How Risky it is:</td><td colspan="3">This poses a medium-level risk for ML/TF/PF activities, because we have to rely on external systems. This risk can be mitigated by applying FIC- required CDD measures along with credit worthiness checks.</td></tr>
<tr><td>Discussion of Threats:</td><td>Threat:</td><td colspan="3">Possible Fabrication of information provided</td></tr>
<tr><td></td><td>How Risky it is:</td><td colspan="3">This poses a medium-level risk for ML/TF/PF activities. This risk can be mitigated by applying strict verification of information policies, as per FIC Requirements</td></tr>
<tr><td>Overall Risk Conclusion:</td><td colspan="2">High</td><td>Neutral</td><td>Low</td></tr>
<tr><td colspan="3">Can the Risk be mitigated / avoided?</td><td>Yes</td><td>No</td></tr>
</table>

Each product and service your firm offers must be rated for risk, and each of these risk analyses and rating must be contained in your RMCP.

**Client-level Risk**

Every Accountable Institution needs to address how they risk-rate their clients. Clients can be risk rated as follows:

1. **Low risk** clients are clients who adhere to **all of** the following criteria**:**
    a. Existing clients or previous clients
    b. With whom identification and verification of identity was possible; and
    c. Whose proof of funds and subsequent receipt of funds was done without threat of contract breaking.
    d. For whom currently valid FICA and CDD documents are still on file (not older than 6 months)
2. **Neutral Risk** clients are clients who have one or more of the following characteristics:
    a. Any Individuals or legal persons with whom there have not been any previous business relationship concluded.
    b. Previous clients whose transactions have concluded more than 6 months ago.
3. **High Risk** clients are clients who have one or more of the following characteristics:
    a. FPEP's (Foreign Politically Exposed Persons) or DPEP's (Domestic Politically Exposed Persons)
    b. Any Individual or legal person supplying funds that is above the thresholds for cash or other transactions as set out by the Financial Intelligence Centre.
    c. Any Other Individual or Legal Person who does not meet the requirements for Low- or Neutral Risk clients as defined above.

Client risk assessments are done by the use of our **FIC Questionnaires**, attached hereto. We use these Questionnaires and the supporting documents we require our clients to provide to do a risk assessment on each client, and to comply with FIC requirements, which allows us to mitigate most risks associates with client-level risk.

We apply **different levels of Customer Due Diligence for each risk level**. Refer to our customer Due Diligence procedures contained in other parts of our RMCP for these CDD procedures.

# 2. Identification, Verification, Risk Mitigation and Recordkeeping

## 2.1. Identification of Prospective Clients

The Financial Intelligence Centre wants you to explain how you determine who a prospective client is. This seems like something that should be self-explanatory, but the purpose of this, among others, is for organisations to indicate where their clients come from.

This section answers the question: Who should we FICA?

Prospective clients are your target audience for whom you create products or services. They haven't bought anything from you yet, but they have become your leads. And they will become your clients when you set up your advertising campaigns correctly.

For example:

1. Anyone who responds to online listings of properties, by use of the following platforms:
    a. Property 24

b. Private Property
c. Facebook
d. Instagram
e. Gumtree
f. Any other property listing platform.

2. Anyone who responds to online Marketing targeted for a specific purpose or otherwise, who wishes to enter into a sale or lease agreement.
3. Anyone who contacts any of our employees in written form or otherwise of the purpose of entering into a single transaction or business relationship (either sales or rentals).
4. Any person who shows up to a show house or open house for the purpose of entering into a single transaction or business relationship (either sales or rentals).

**For the purposes of clarity, the easiest way to describe this, is that a prospective client is anyone who:**

**WANTS to enter into a Mandate**
**WANTS to enter into a lease agreement**
**WANTS to enter into a Sale Agreement / Offer to purchase**.

## 2.2. Transaction Thresholds (cash and small transactions)

### *2.2.1. Cash Transaction Thresholds*

Your RMCP must contain your procedure for handling the Cash Transaction Thresholds.

The current Cash transaction threshold is **R 49 999.99.**

**What is considered a cash transaction?**

A Cash transaction is any transaction where:

- You receive physical cash in hand for any transaction
- Where cash is deposited into your business' account, visible by some form of CASH DEPOSIT in the description of the transaction on your bank statement.

**What does this entail?**

All cash transactions above the above amount (so R50 000.00 and above) received must be reported to the Financial Intelligence Centre.

It is no longer a requirement to report aggregated amounts received for a single transaction by the same person to FIC, just single amounts.

**What to do when a transaction is over the threshold:**

When a transaction takes place where the cash received is over the threshold, a Cash Transaction Report (CTR) must be made to the Centre, via the FIC GoAML portal.

FIC requires a lot of details to be submitted when making this report, so it is important to ensure your Due Diligence procedures are thorough, so you have the information at hand.

**What must be in you RMCP:**

You need to describe in your RMCP, in relation to the Cash transaction threshold, the following:

- What the current threshold is
- What you will submit as part of the CTR
- What the internal office procedure is for report making.

Any other requirements your office has in relation to transactions where the threshold is exceeded, for example, that the client is considered higher risk, so additional Due Diligence will take place.

#### *2.2.2. Single transaction Threshold for amounts under R5000*

**What is considered a single transaction below R5000?**

- Single transactions (once-off, with no reasonable expectation of having repeat business with the client)
- Transaction is worth less than R5000.00

**What does this entail?**

All single transactions below R5000 need not have full Customer Due Diligence procedures applied.

In Simple terms, you must have basic information on the client so you mitigate the risk of doing business with an anonymous client, but you are not required to verify the information provided.

This is known as Abbreviated CDD – you just need these clients to complete your FIC form and provide a copy of their ID, but they need not supply further information and you do not need to verify the information provided.

**What must be in you RMCP:**

You need to describe in your RMCP, in relation to the Single transaction threshold, the following:

- What the current threshold is
- An explanation of your abbreviated CDD procedures.

## 2.3. Identification and verification of Natural persons

Your RMCP should describe how your office identifies and verifies natural persons.

This is where you will be able to reference your risk rating methodology for client-level risk assessments.

The basic requirements as per the FIC Act is as follows:

| Type | Document(s) Required | Verification Method |
|---|---|---|
| South African Citizen | • A clear copy of their ID documents (both sides of the ID card, if it is the card) | The agent / staff member will request to see their actual ID document in person to verify if it belongs to the intended person.<br><br>ID verification can also be done via online portals, such as banks and credit bureaus. |

| | | |
|---|---|---|
| Non-South African Citizen | • A clear copy of a valid Passport and work permit | The Agent / staff member will request to see their identification documents in person to verify if it belongs to the intended person. |
| If the Natural person operates through a representative (for both SA and non-SA citizens) | • Either a copy of their passport and / or ID document, depending on their citizenship, for both the intended client and the representative.<br>• A Proxy letter / declaration explaining the nature and power of the representative i.r.t. the transaction.<br>• Contact details of the person whom the representative is representing. | The Agent / staff member will request to see their identification documents in person to verify if it belongs to the intended person.<br><br>The Agent / staff member would contact the intended client via contact details provided to verify if the information provided and intentions of the representative are correct. |

Further requirements as per the FIC Act:

| **Sales** | **Rentals** |
|---|---|
| For Purchasers:<br>• Proof of income<br>• Current proof of address (in the form of a bill)<br>• Marriage Certificate (to establish in-community marriages) | For Lessees:<br>• Proof of income (both in the form of a payslip and bank statement)<br>• Current Proof of Address (in the form of a bill)<br>• A filled-out application form, for establishing work details and the like.<br>• A credit rating report (to be drawn by the agency to ensure credit-worthiness) |
| For Sellers:<br>• Current proof of address (in the form of a bill)<br>• Proof of ownership of property intended to be sold, either in the form of a municipal not older than 3 months, or a property report from Lightstone / Windeed.<br>• Marriage Certificate (to establish in-community marriages) | For Lessors:<br>• Current proof of address (in the form of a bill)<br>• Proof of ownership of property intended to be Let, either in the form of a municipal bill, not older than 3 months, or a property report from Lightstone / Windeed.<br>• Marriage Certificate (to establish in-community marriages) |

Then, to apply your Risk-rating matrix, the following will apply:

| Risk Level | Difference in Identification and Verification requirements |
|---|---|
| **Low-Risk Clients** | No FIC docs needed if already on file and not older than 6 months |
| **Neutral-Risk Clients** | The exact documents as listed above required at all times. |
| **High-Risk Clients** | All identification documents must be certified by a Police Commissioner of oaths, and a Declaration in affidavit-form must be given to ensure the accuracy and validity of the documents provided for identification and verification purposes. |

## 2.4. Identification and Verification of Legal Persons

Your RMCP should describe how your office identifies and verifies Legal persons.

For the purposes of FIC, we classify Trusts and Partnerships as legal persons, as beneficial ownership must also be determined.

This is where you will be able to reference your risk rating methodology for client-level risk assessments.

**Identification / Verification methods for the legal persons:**

| Type | Document(s) Required | Verification Method |
|---|---|---|
| Private Company (Pty) ltd | • A Signed copy of their Company Registration documents as extracted from the CIPC website<br>• Share Certificate indicating ownership percentages | The information provided by the registration documents i.r.t directors and other info, can be verified by visiting the CIPC website, or via credit bureau's such as TPN. |
| Close Corporations (CC's) | • A Signed copy of their registration documents as extracted from the CIPC website<br>• Share certificate indicating member ownership percentages | The information provided by the registration documents i.r.t members and other info, can be verified by visiting the CIPC website, or via credit bureau's such as TPN. |
| Partnerships | • Fully Signed Partnership Agreement / certificate of Incorporation | The Partnership agreement can be verified by requesting that the documents get certified by a Commissioner of Oaths |

| | | |
|---|---|---|
| | • Share certificate indicating profit share margin for each partner | |
| Trusts | • Trust Deed<br>• Trust Authorization letter issued by the government | The Trust Deed and authorization letter can be verified by enquiring with the deeds office if the information provided is correct. |

**What Identification / verification documents to gather for all beneficial owners:**

The Following list of documents must be gathered to determine the beneficial owners of the above persons, and must accompany the company identification documents at all times:

1. Clear copies of the identification documents of all members / directors / partners / trustees as appearing on the identification documents and share certificates.
2. Proof of residences for the legal person and all its members / directors / partners / trustees.
3. 6 Months bank statements of the legal person, and management financial statements for 6 months. (This is only needed in the case of Purchasers and Lessees)
4. Proof of ownership of the property concerned, in the form of a municipal bill not older than 6 months, or a property report extracted from Lightstone or Windeed.
5. A Resolution by all members / directors / partners / trustees to explain who will be representing the legal person / trust / partnership during the transaction, what their powers and limitations are i.r.t the transaction / business relationship, and the intended purpose of the transaction / business relationship being entered into.
6. The documentary requirements for non-SA citizens as captured in the natural person section must be applied if any of the members / directors / partners/ trustees are not a South African Citizen.

**Applying your Risk Rating:**

| **Risk Level** | **Difference in Identification and Verification requirements** |
|---|---|
| **Low-Risk Clients** | No FIC docs needed if already on file and not older than 6 months. |
| **Neutral-Risk Clients** | The exact documents as listed above required at all times. |
| **High-Risk Clients** | All identification documents must be certified by a Police Commissioner of Oaths, and a Declaration in affidavit-form must be given to ensure the accuracy and validity of the documents provided for identification and verification purposes. |

### *2.4.1. Beneficial Ownership*

**NB: This Obligation has changed with Guidance note 7A – thus if you have an RMCP already in place, please make sure to update this section**

For all legal entities, Partnerships and trusts, the Act specifies that ultimate beneficial ownership must be determined.

**Who is a Beneficial owner?**

*(a) means a natural person who directly or indirectly–*

*(i) ultimately owns or exercises effective control of–*

*(aa) a client of an accountable institution; or*

*(bb) a legal person, partnership or trust that owns or exercises effective control of, as the case may be, a client of an accountable institution; or*

*(ii) exercises control of a client of an accountable institution on whose behalf a transaction is being conducted; and*

*(b) includes–*

*(i) in respect of legal persons, each natural person contemplated in section 21B(2)(a);*

*(ii) in respect of a partnership, each natural person contemplated in section 21B(3)(b); and*

*(iii) in respect of a trust, each natural person contemplated in section 21B(4)(c), (d) and (e);*

**We are therefore looking for all Natural Persons who benefits from the entity financially, and / or holds a controlling interest in the entity.**

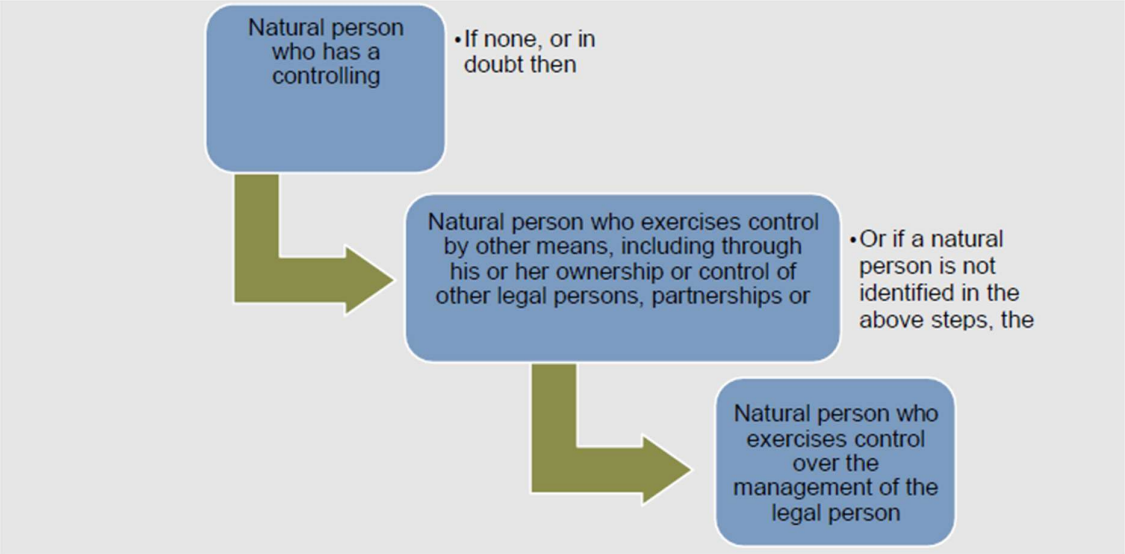
**How to identify a beneficial Owner**

| **Type of Entity** | **Beneficial Owners** |
|---|---|
| Private Company (Pty) Ltd / Public Company Ltd's / Inc's | • All Directors<br>• Shareholders who own more than 5% equity in the business (shares, options, etc) |
| Close Corporation CC's | • All Members |
| Partnerships | • All Partners |
| Trusts | • Trust Beneficiaries<br>• Trustees |

If any entity has a Director / member / partner that is also a legal person, you must continue to determine who the Natural Persons are who exercise control over the entity.

The FIC has identified the following process of elimination:

(Financial Intelligence Center, 2024)




**Please reference PCC 59 for further guidance on determining Beneficial Ownership**

All Beneficial Owners must complete the Identification and verification paperwork as with any other natural person.

## 2.5. Customer Due Diligence – Order of Attempts, when it must be concluded, what happens when it is not concluded, and how termination of business relationships occur.

Your RMCP must describe the timeline of how CDD is done in your business.

**What is Customer Due Diligence?**

Customer Due Diligence is the HOW of FICA – meaning, how do we identify and verify our clients? By applying Customer Due Diligence. This is a concept, rather then a clearly definable term, and is about the process you use when identifying and verifying your clients.

**Timing of CDD:**

| Type of Client | When CDD Documents are requested | Who completes CDD? | When CDD Should be Completed |
|---|---|---|---|
| Lessors | CDD documents are requested when the client indicates their intent to enter into a transaction / business relationship. In plain terms, **when the lessor enters into a** | The agent is responsible for compiling and submitting the CDD documents to the office, after which the rental administrator who processes the mandate verifies the | CDD Documents and the verification thereof **should be completed before marketing starts**. In plain terms, before a property listing is made live on advertising platforms. |

| | | | |
|---|---|---|---|
| | **mandate** with one of our agents / office. | documents submitted and performs the needed checks. | |
| Lessees | CDD documents are requested when the client indicates their intent to enter into a transaction / business relationship. In plain terms, **when the lessee enters into a lease agreement** with one of our agents / office. | The agent is responsible for compiling and submitting the CDD documents to the office, after which the rental administrator who processes the lease agreement verifies the documents submitted and performs the needed checks. | CDD Documents and the verification thereof **should be completed before the lease agreement is finalised**. In plain terms, before a lease agreement is signed and finalised. |
| Sellers | CDD documents are requested when the client indicates their intent to enter into a transaction / business relationship. In plain terms, **when the seller enters into a mandate** with one of our agents / office. | The agent is responsible for compiling and submitting the CDD documents to the office, after which the rental administrator who processes the mandate verifies the documents submitted and performs the needed checks. | CDD Documents and the verification thereof **should be completed before marketing starts**. In plain terms, before a property listing is made live on advertising platforms. |
| Buyers | CDD documents are requested when the client indicates their intent to enter into a transaction / business relationship. In plain terms, **when the buyer makes a bona fide offer to purchase** with one of our agents / office. | The agent is responsible for compiling and submitting the CDD documents to the office, after which the rental administrator who processes the mandate verifies the documents submitted and performs the needed checks. | CDD Documents and the verification thereof **should be completed before the offer to purchase is submitted for consideration**. In plain terms, before the offer is submitted to the seller for consideration. |

**Order of Attempts for CDD to take place:**

The FIC expects of you to explain what order of attempts you take in trying to complete Customer Due Diligence. Here follows standard procedure for the order of attempts:

- Step 1: The Property Practitioner who is facilitating the business relationship / transaction requests the documents as per the table above.
- Step 2: If the client fails to produce the documents upon the Property Practitioner's request, the Property Practitioner will request in a formal email 2 business days after the initial request, for the documents to be submitted.
- Step3: If the client fails to produce the documents after the second request, the office administrator responsible for processing the transaction will request for a third time in writing for the client to submit the documents, no later than 2 business days after the second request made by the Property Practitioner.

When all 3 steps above have been followed, and the client still fails to produce the required CDD documents, it can be safely deduced that CDD procedure will not be able to be completed. In this case, the transaction / business relationship must be terminated.

**How Business relationships / Transactions are terminated if CDD cannot take place?**

The first step that must take place when CDD cannot be completed, is that the client must be informed that the business relationship / transaction may not move forward if the appropriate CDD procedure is not completed. This will be done in writing in the form of an email by the Administrator involved.

After the client has been informed, any documents that were signed prior to the conclusion of the CDD procedures which gave rise to any obligation on the part of the Property Practitioner or any other party must be officially cancelled, in writing, in the form of a cancellation notice.

The last step that must be followed is that a Suspicious Transaction Report must be submitted. The same steps as outlined on our Suspicious transaction section of our RMCP will be followed in this regard.

**Ensuring you do not do business with clients who operate under a false or fictitious name:**

The standard CDD documents and processes as described above eliminates most risk of doing business with someone with a false / fictitious name. Although not all risk can be mitigated or known, all the procedures put in place ensures that you follow all reasonable steps to ensure you do not do business with someone who has a false name.

## 2.6. Doubts About Veracity of Previously Obtained Information

Another word for veracity is Accuracy or legitimacy. Your RMCP must describe what you would do if you have suspicions that your client's submitted paperwork is not accurate / fraudulent.

Section 21D of the FIC Act Clearly states:

'When an accountable institution, subsequent to entering into a single transaction or establishing a business relationship, doubts the veracity or adequacy of previously obtained information which the institution is required to verify as contemplated in sections 21 and 21B, the institution must repeat the steps contemplated in sections 21 and 21B in accordance with its Risk Management and Compliance Programme and to the extent that is necessary to confirm the information in question.'

**Additional Steps to take:**

Here are examples of extra steps you can take to verify the information provided:

1. The Property Practitioner conducts the FIC Questionnaire verbally with the client, and cross-checks if the information written down on the FIC Questionnaire and the information given verbally corresponds with each other.
2. The Property Practitioner runs an ID verification on the client via TPN, to check if the ID copy provided and the person they work with, matches.
3. The Property practitioner requests a bank confirmation letter from the client, which can be used to run a verification check if the bank details correspond with the true account holder.
4. The Property Practitioner contacts the client's employer to verify their client's particulars as provided on their payslip.

If the information provided proves to be false / does not correspond with what you believed to be true about the client, you must follow your Suspicious / Unusual Transaction procedures to report the matter to FIC, and end the Business relationship / single transaction.

## 2.7. Section 21A of the FIC Act

Your RMCP must describe how and where your paperwork determines and describes :

a. The Nature of the business relationship concerned.
b. The Intended purpose of the business relationship concerned.
c. Source of funds to conclude transaction.

This is an easy section, because your contract documents should already have specific clauses that describes these items. You can therefore just refer to the clauses where these items are described in your contract documents.

For source of funds, your FIC Questionnaire and its accompanying documents will be the documents to determine the source of funds.

## 2.8. Complex and unusually Large Transactions

Your RMCP must describe what your firm considers to be normal transactions, and what happens when transactions are more complex or unusually larger than what you consider normal. Recordkeeping of these transactions should also be described.

**For example:**

Normal transaction Range based on value:

| **MINIMUM** | **MAXIMUM** |
|---|---|
| **SALES TRANSACTIONS** | |
| R 550 000 | R 5 000 000 |
| **RENTALS TRANSACTIONS** | |
| R 5000 | R 30 000 |

Normal transaction in terms of complexity:

1. No more than 2 co-signers for each end of the transaction.
2. No more than 1 suspensive or resolutive condition for sales transactions.
3. No more than 2 payments involved for the source of funds of buyers.
4. No more than 2 transactions linked by way of suspension conditions at a time.

**Any transactions that fall outside of these parameters, must be categorised as automatically high risk, and must be reported to the Financial Intelligence Centre as a Suspicious transaction.**

## 2.9. Suspicious or Unusual Transactions

Your RMCP must contain a section explaining what you consider a suspicious or unusual transaction.

Let's talk about what gives rise to the obligation to report these types of transactions:

An Accountable Institution must report their knowledge or suspicion to the Financial Intelligence Centre whenever:

- They become aware of something,
- Circumstances arise in which a person can reasonably be expected to be aware of something or,
- Circumstances arise in which a person can reasonably be expected to suspect something.

These activities can relate to any situation which concerns our company, transactions where our company is involved, or are a party to, which includes:

- Where the business has received proceeds of unlawful activities, or is about to receive such proceeds,
- Where the business has received property which is connected to an offence relating to financing of terrorist activities, or is about to receive such property,
- Were the business has been used in any way for money laundering purposes, or is about to be used for money laundering purposes or,
- Where the business has been used in some way to facilitate the financing of terrorist activities or is about to be used for this purpose.

Business Activities that are deemed as suspicious include transactions with the business where the transaction:

- facilitated the transfer of proceeds of unlawful activity or is likely to do so,
- facilitated the transfer of property which is concerned to an offence relating to financing of terrorist activities or is likely to do so,
- does not appear to have a business purpose,
- does not appear to have a lawful purpose,
- may be relevant to the investigation of tax evasion by SARS,
- somehow relates to an offence relating to financing terrorist activities.

Accountable Institutions are only required to report in connection with the **proceeds of unlawful activities** and **money laundering** or **terror financing** offences, **and not general criminal offences.**

**Indicators of Suspicious or Unusual transactions:**

It is important to firstly have your agents rely on their instincts. Suspicions are subjective in nature, but here are some indicators to look out for:

**Unusual Business:**

- Deposits of funds with a request for their immediate transfer elsewhere
- Unwarranted and unexplained international transfers
- The payment of commissions or fees that appear excessive in relation to those normally payable
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type of transaction or particular method of transacting
- Transactions do not appear to be in keeping with normal industry practices
- Purchase of commodities at prices significantly above or below market prices
- Unnecessarily complex transactions
- Unwarranted involvement of structures such as trusts and corporate vehicles in transactions
- A transaction seems to be unusually large or otherwise inconsistent with the customer's financial standing or usual pattern of activities
- Buying or selling securities with no apparent concern for making a profit or avoiding a loss
- Unwarranted desire to involve entities in foreign jurisdictions in transactions.

2. **Knowledge of Reporting or Record keeping Requirements**

- A customer attempts to convince employee not to complete any documentation required for the transaction
- A customer makes inquiries that would indicate a desire to avoid reporting
- A customer has unusual knowledge of the law in relation to suspicious transaction reporting
- A customer seems very conversant with money laundering or terrorist activity financing issues
- A customer is quick to volunteer that funds are clean or not being laundered.

3. **Identification**

- The use of a seemingly false identity in connection with any transaction, including the use of aliases and a variety of similar but different addresses and, in particular, the opening or operating of a false name account
- Opening accounts using false or fictitious documents
- A customer provides doubtful or vague identification information
- A customer refuses to produce personal identification documents
- A customer changes a transaction after learning that he must provide a form of identification
- A customer only submits copies of personal identification documents

- A customer wants to establish identity using something other than his or her personal identification documents
- A customer's supporting documentation lacks important details such as contact particulars
- A customer inordinately delays presenting corporate documents or
- All identification presented is foreign or cannot be checked for some reason.

4. **General**

- A customer provides insufficient vague or suspicious information concerning a transaction
- Accounts that show unexpectedly large cash deposits and immediate withdrawals
- A frequent exchange of small denomination notes for larger denomination notes
- Involvement of significant amounts of cash in circumstances that are difficult to explain.

**Closing of Accounts**

- The act of closure of an account may not be suspicious, but the specific context of the closure of account must be considered when deciding if it must be reported to the Centre or not.

**Process for submitting an STR to the Centre:**

STR's must be submitted within 5 days of becoming aware of the suspicion, via the FIC website, using the form provided on the FIC website. STR's may not be posted.

STR's may also be batch-reported if the need arises, if the Institution regularly reports STR's to the Centre.

The following information must be contained in an STR:

- The Person or entity making the report
- The Transaction being reported
- Any account involved in the transaction
- The person conducting the transaction or the entity on whose behalf it is conducted
- General information concerning the transaction.

## 2.10. Copy of Sec 21 and 21B of the FIC Act

Your RMCP should contain a copy of Section 21 and 21B of the FIC Act.

This can literally be copied and pasted into your file.

These sections are the FIC's minimum rules for identification and verification, which was covered in Part 2 of our course.

## 2.11. FPEP's and DPEP's

**What are FPEP's and DPEP's?**

And FPEP is a Foreign Politically exposed person, and a DPEP is a Domestic Politically exposed person.

These terms used to be FPIP's and DPIP's, which stood for prominent influential persons, but has since been updated by FIC.

Who qualifies as FPEP's and DPEP's?

Someone who has held in the last 12 months any of the following positions:

Foreign:

- Head of state of a country or government
- Member of a foreign royal family
- Government minister of equivalent senior Politian or leaser of a political party
- Senior judicial official
- Senior executive of a state-owner corporation
- High-ranking member of the military

Domestic:

- The president or deputy president
- A government minister or deputy minister
- The premier of a province
- A member of the executive council of a province.
- Executive mayor of a municipality
- Leaders of political parties
- Senior traditional leaders
- The CEO, CFO or accounting officer of a national or provincial department or government component
- Municipal managers or CFO's
- The board members and CEO, or CFO of a publicly listed entity.
- Judges in any level of court
- Ambassadors or high commissioners for other governments
- High-ranking military members
- The CEO and CFO of any Company who provides services or products for organs of state (tenders, etc)
- An executive of an international organisation based in SA.

For both domestic and foreign PEP's, it also includes family members and known close associates:

- Spouses, civil partners or life partners
- Ex-partners
- Children and stepchildren
- Parents

- Siblings or step siblings and their spouses

**How to identify a PEP:**

Your FIC questionnaire will be your guidance document for determining if someone falls into these categories.

You ask outright if someone is one of these categories on your questionnaire. The FIC does not expect you to become an investigator just to determine if each client falls in this category, as long as you have asked outright, and do not have reason to believe they might be lying, then you have done your Due Diligence.

If someone answers on their FIC questionnaire that they are one of the categories listed, or you have reason to suspect that they were not truthful of their status on their FIC questionnaire, then you can take additional measures to screen a client, by visiting various websites and doing a search on their name.

**Procedures for PEP's:**

FIC outlines in Section 21F of the FIC Act, that if someone is found to be a PEP, the following procedures must be followed:

- Obtain senior management approval for establishing the business relationship
- Take reasonable measures to establish the source of wealth and source of funds for the client
- Conduct enhanced ongoing monitoring of the business relationship.

Someone being a PEP does not automatically mean you have an obligation to report to the FIC, but if they are even a little bit suspicious, or you struggle to ascertain their source of funds, then you must make a Suspicious Transaction report.

You can decide, based on your Risk Apatite, if you want to do business with a PEP.

## 2.12. TFS Screening

The FIC expects of us to screen every prospective client on the Targeted Financial Sanctions list, as part of your CDD measures.

**What is the TFS List?**

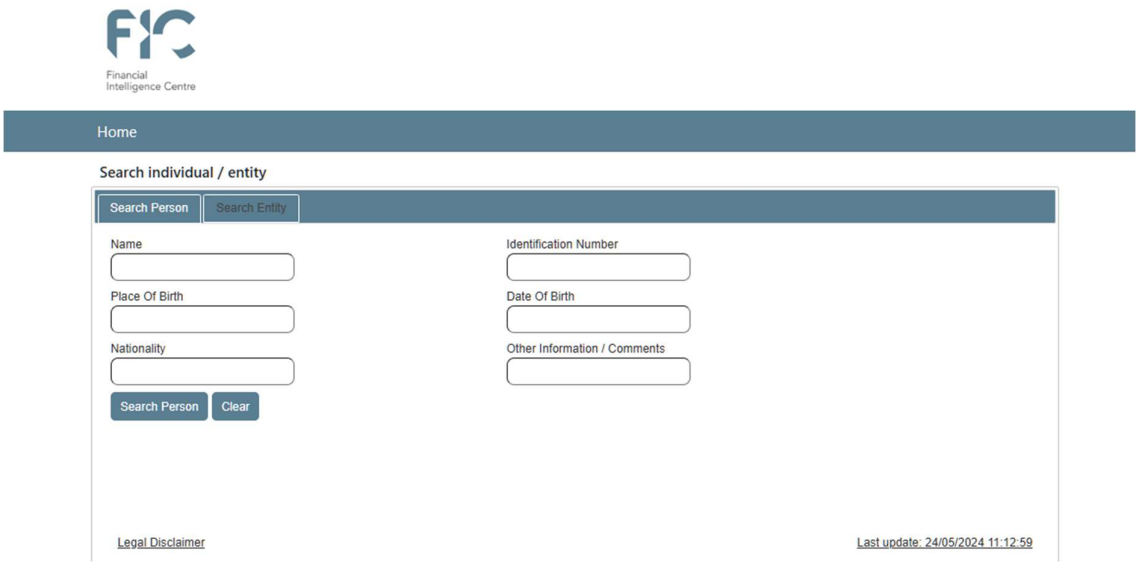
The Targeted Financial Sanctions list is a consolidated list of all persons and entities that we as a country have Financial and administrative sanctions against. Entities and individuals on this list either:

- Participated in Terrorist activities
- Participated in Money laundering activities
- Are from countries on the UN and Financial Action Task Force Black list
- Are from countries on which our country has a sanction against.

**How do we screen client against this list?**

The FIC has a website and a search tool you can use to screen clients against this list. This website can be accessed here:

https://tfs.fic.gov.za/Pages/Search




You then enter al the details you have for the client as provided on their FIC questionnaire, and click 'search person'.

The Best result is a no-result. A no-result means that the person or entity is not on the TFS list, and you can continue as normal.

If you get a positive hit, you need to consider the following factors:

- Is it a full match, with name and place of birth?
- Is it a partial match, based on place of birth or citizenship?

If you have a full match, you must make a Terrorist Financing Activity Report (TFAR) with the FIC, and immediately cease doing business with the client.

If you have a partial match only based on country of origin, you can decide if you want to proceed with a business relationship or not, based on context, and your own risk appetite.

**Updates on the TFS List:**

The FIC updates the TFS list every now and then, and issues a notice that an update on the TFS list has occurred.

When such a notice is issued, you are required to re-screen all your active clients against the TFS list again, to ensure they have not since been added to the list.

Ensure you are subscribed to receive these updates, so you don't miss it, here:

https://tfs.fic.gov.za/Pages/Subscriptions

**What to put in your RMCP in relation to TFS List screening:**

You must include in your RMCP:

- Your screening procedure

- Reporting procedure for positive results
- How you freeze assets where you may have assets in your possession.

## 2.13. Proliferation Activities and Weapons of Mass Destruction

The Financial Intelligence Centre Published PCC No 54 to offer guidance on combating Proliferation Financing, and Accountable Institutions as required to comply with this Notice. Accountable Institutions are not required to monitor the act of terrorism or proliferation itself, but rather the financing thereof through the use of the Accountable Institution's services.

**What are Proliferation Activities and Weapons of Mass Destruction?**

The Non-Proliferation of Weapons of Mass Destruction Act 87 of 1993 defined WMD as:

"... any weapon designed to kill, harm or infect people, animals or plants through the effects of a nuclear explosion or the toxic properties of a chemical warfare agent, or the infectious or toxic properties of a biological warfare agent, and includes a delivery system exclusively designed, adapted or intended to deliver such weapons."

The Financial Action Task Force (FATF) defines Financing of proliferation of WMD as:

"... the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)"

Proliferation financing risk is defined by the FATF as:

"... the potential breach, non-implementation or evasion of the targeted financial sanctions"

Thus, Proliferation Financing of WMD is confined to instances where funding is made available to persons on the TFS list.

**How do I identify if a client is involved in these activities?**

The FIC, once again, does not expect us to become investigators to determine these things. It is sufficient for Accountable Institutions to use the TFS list screening to this end, the same procedure followed here, can be used to this end. Your TFS list screening will cover this for you.

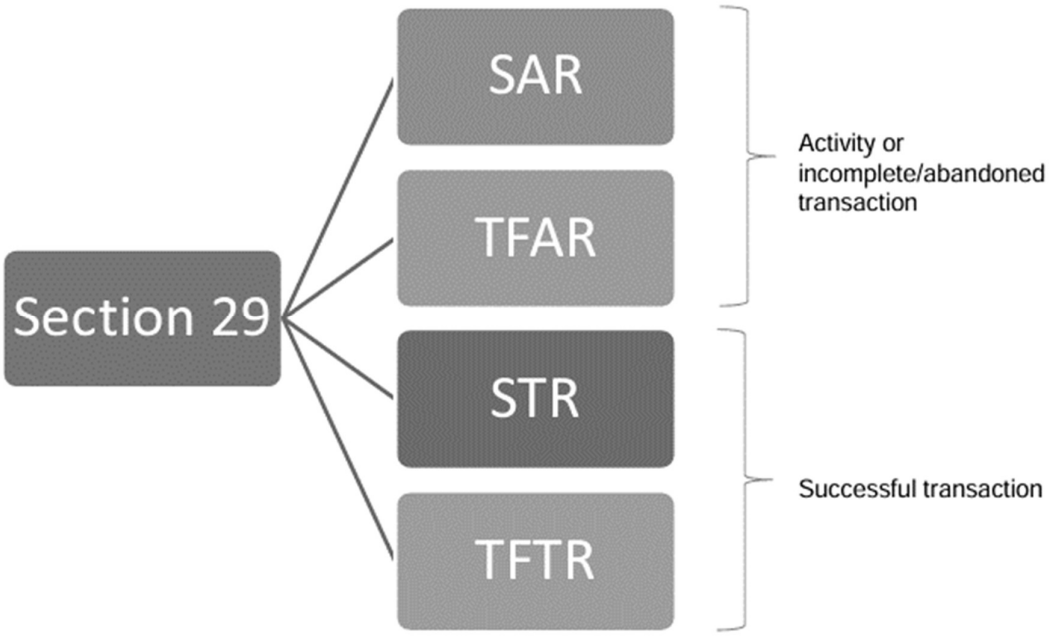
**What to put in your RMCP in relation to Proliferation and WMD:**

- Discuss the concepts, to show your understanding
- Mention that you will use your TFS list screening to this end as well.
- Office procedure for reporting.

## 2.14. Obligation to make reports / Reporting Procedure

The FIC expects Accountable institutions to make reports whenever the obligation arises.

The different types of reports that you can make, are:




And then as well:

- Cash Transaction Reports (CTR's)
- International Transaction reports (ITR's)

**Timing of reports:**

| **Type of Report** | **By When the Report must be made** | **When obligation to report arises** |
|---|---|---|
| Cash Threshold Report (CTR) | Within **2 Business days** of receipt of the cash amount exceeding the Cash Threshold. | Cash Receipt on business premises exceeding R49 999;<br><br>Cash deposited into bank account exceeding R49 999. |
| Suspicious and Unusual Transaction Reports (STR's) | Within **5 business days** of suspicion arising. | Suspicion of ML/TF/PF arises,<br><br>Unusual Transaction pattern with no lawful purpose,<br><br>Refer to Suspicious transaction policy in RMCP. |
| Terrorist Financing Transaction Reports (TFTR's) | Within **5 days** of positive hit on TFS list Search | When client screening returns positive result for presence on Consolidated TFS List. |

**Standard Procedure for Report Making:**

| Step | Action |
|---|---|
| 1 | Once the obligation to report arises, the staff member who became aware of the obligation to report, makes record of their findings, as per the guidelines contained in our RMCP. |
| 2 | The staff member reports their findings to the FIC Compliance Officer within 24 hours, and supplies them with their findings, and all other paperwork relevant to the transaction / business relationship. |
| 3 | The FIC Compliance Officer receives the findings and paperwork by the staff member, and does further due diligence to ensure they have all the needed information to lodge a report with FIC, including interviewing the staff member who became aware of the obligation to report. |
| 4 | The FIC Officer lodges the relevant compliant with the FIC using their GoAML Portal login details. |
| 5 | The FIC Officer files the report made, along with all paperwork and findings that accompany the report, in a separate filing system, and await further instruction from the FIC where applicable. |

**Informing your client a report has been made:**

There is a delicate balance of what may be shared with a client against which a report has been made, and what may not be shared.

The client must be informed in cases where:

- The transaction / business relationship cannot continue because of the circumstance that caused the report to be made (for example a TFS list hit)
- The client's assets have been frozen.

In any circumstance where the transaction moves forward, for example with the cash threshold or with Politically exposed persons, the client does not need not be informed of the report being made.

## 2.15. Record Management Process

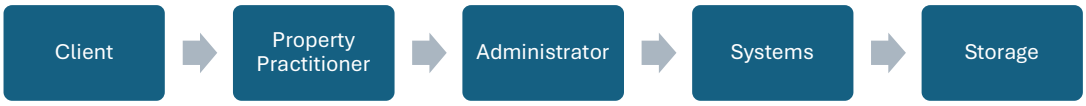
FIC Expects of Accountable Institutions to keep thorough records of transactions and business relationships.

When you align your record management process with FIC's rules, you must think of the following:

- How is contract and FIC documents collected from clients, and who is responsible for this?
- How is contract and FIC documents collected from agents, and who is responsible for this?
- Who checks contract and FIC documents of transactions, and follows up with responsible parties when they are not sufficient / correct?
- How is contract and FIC documents and information captured in the firm's internal systems, and who is responsible for this?
- How and where are records kept of all transactions?

**Record Management must be kept in mind at all stages of a contract because it is the only evidence that will remain of a transaction, after it has been concluded.**

**The Flow of information:**




Make mention of the flow of information and records in your firm, in the form of a flow chart.

You must also make sure that you mention, in detail:

- All systems used for record storing purposes
- The security measures to ensure the safety of the records.
- How long you keep records (minimum 5 years)

It is important to ensure your RMCP thoroughly describes your Record management process.

## 2.16. Section 42 of the FIC Act

The FIC expects of Accountable Institutions to specifically mention which clauses in Section 42 of the FIC Act applies to them, and which not.

You can do this via a checklist, and for the items you believe is not applicable to you, you must explain why it is not applicable.

Sections A-P and R and S will always Apply. Section Q only applies to firms where they have branches and subsidiaries and are not independently owned and operated.

## 2.17. Employee Screening

The FIC issued Directive 8 in 2023, saying that Accountable Institutions must screen all their employees as well. This screening is compulsory.

The following steps must be followed when screening employees:

**Step 1: Risk Rating of Job Description and responsibilities**

Do a risk rating for all job titles currently held in your company. This can be done in the following format:

| | |
|---|---|
| **Job Title** | |
| **Job Description** | |

| | |
|---|---|
| **Job Responsibilities** | |

| | YES | NO |
|---|---|---|
| Does this job include screening prospective clients for Money Laundering /Terrorist Financing Activities? | | |
| Does this job include doing Customer Due Diligence (CDD) to decide if a prospective client may be onboarded or not? | | |
| Does this job include having full unencumbered access to confidential client information? | | |
| Does this Job include having access to the firm's bank accounts, including but not limited to any Trust Accounts? | | |
| Does this Job include making decisions that impact the firm's CDD and KYC (Know Your Client) procedures? | | |
| Is this job considered to form part of the Top level of the management structure of the firm? | | |
| Will the person appointed in this position be a beneficial owner of the firm? (holding shares or profit share) | | |
| | | |
| If any of the above questions have been answered YES, this job is considered to be high-risk, and Employee screening should happen on an ongoing basis, at least once a year. | | |
| If all questions are answered NO, this position is considered to be low-risk, and employee screening can take place when onboarding new employees. | | |

**Step 2: Have Employees complete a FIC Questionnaire specifically designed for Employees, focussing on Integrity, competency and Screening for Political exposure and TFS.**

The template will be provided, for ease of reference.

**Step 3: Record keeping**

Keep the results of the screening on file for employees, for at least 5 years OR as long as the employee works for you, whichever comes first.

Employees must be re-screened as with clients on the TFS list, and the rest can be re-screened at your discretion.

# 3. Training

## 3.1. Training

All Accountable Institutions must ensure their employees are properly and regularly trained on FIC Concepts.

Employees must be trained on general FIC Concepts, and your firm's RMCP.

What to include in your RMCP related to Training:

- Proof of training materials
- Proof of attendance of employees
- Training schedule for employees

When FIC conducts an inspection, they will check that training was conducted at regular intervals.

## 3.2. Contract Documents

The last thing you must add in your RMCP, is the templates your office uses for all its contracts.

This includes:

- Sale Agreements
- Rental Agreements
- Questionnaires
- Mandates
- Mandatory Disclosure forms
- Addendums
- Internal documents used to facilitate contracts

## 3.3. General Considerations when drawing up your RMCP:

These are general recommendations and obligation sunder the Act, as it relates to your RMCP:

- Your RMCP should be readily available for employees to access, as well as for inspection purposes.
- If you make reference to a document in your RMCP, annex it to the RMCP. If it is not reference or annexed onto the RMCP, it does not form part of the RMCP.
- When considering a FIC Compliance Officer for your office, please ensure they have relevant seniority and expertise on Compliance matters.

# Submission of your RMCP by 12 March 2025

All Accountable Institutions must submit the latest version of their RMCP on their GoAML Portal by no later than 12 March 2025.

**Submission Specifications:**

- The Document must be submitted in PDF Format
- The File Name must be in the following format: YYYYMMDD – RMCP. The Date used must correspond with the date of last revision. (example – 20250310 – RMCP)

**Submission steps:**

1. Log onto the GoAML Portal with your login details
2. Click on the 'MyGoAML' drop-down menu
3. Click on 'My Org Details'
4. Scroll down to the 'Attachment' section, and click on 'Upload'
5. Select the document from your computer from here, and click 'Open'
6. Click on 'Submit Request'
7. Click on 'Continue'

While you are on your GoAML portal, ensure you update your address and contact details!

# Common Non-Compliance in FIC Inspections

The following items have been identified by the FIC as common non-compliance findings during FIC Inspections:

- Non-submission of Directive 6 RCR's
- No RMCP's or the use of insufficient 'templates' which have not been made unique to the firm.
- There are no Risk assessments in the RMCP for the business
- The registration / contact details of the firm is not updated on their GoAML Portal
- The determination of Beneficial Ownership for legal entities in firms is not sufficient.
- The firm is not screening all clients against the TFS list / cannot provide evidence that screening has been done.