STRENGTHENING LEGAL PRACTICE: IMPLEMENTING EFFECTIVE RISK MANAGEMENT AND COMPLIANCE PROGRAMMES TO COMBAT FINANCIAL CRIME

Operating in an increasingly complex financial landscape, legal practitioners play a vital role in upholding the integrity of the profession and protecting the broader economy from financial crime.

Listed as accountable institutions in the updated Schedule 1 of the Financial Intelligence Centre Act (FIC Act), legal practitioners admitted and enrolled under the Legal Practice Act are within scope and are required to develop, document, maintain and implement a risk management and compliance programme (RMCP) for combating money laundering (ML), terrorist financing (TF) and proliferation financing (PF).

Developing and implementing an RMCP is an essential starting point for legal practitioners when applying a risk-based approach to combating money laundering and terrorist financing. An effective RMCP should also address PF risk and beneficial ownership controls where clients are legal persons, trusts or partnerships.

The technical requirements for RMCPs are set out in section 42 of the FIC Act. An RMCP that does not adhere to the technical requirements will render the institution non-compliant. Current FIC guidance on RMCPs is consolidated in Revised Guidance Note 7A (2025), which replaces prior versions of GN 7 and GN 7A

Developing an RMCP

An RMCP captures the institution's assessment and understanding of their risk profile in terms of exposure to ML, TF and PF. In addition, the RMCP details what measures the institution will take to identify, assess, monitor, manage and mitigate these risks. The FIC issued public compliance communications (PCC) 53 which offers guidance on developing an RMCP, and includes a simplified guidance template. Practitioners should also consult Revised Guidance Note 7A for the latest expectations on RMCP governance, documentation and approval.

The RMCP must address all the requirements outlined in section 42 of the FIC Act and this includes:

- RMCP governance (including approval by the person(s) exercising the highest level of authority)
- ML, TF and PF risks assessment and risk-rating framework
- Customer due diligence controls

- Additional due diligence controls
- Targeted financial sanctions controls aimed at terrorist and proliferation financing (implementation in terms of sections 26A–26C read with POCDATARA and PCC 44A)
- Prominent person controls for Domestic Prominent Influential Persons (DPIPs) and Foreign Prominent Public Officials (FPPOs)
- Transaction monitoring
- Reporting controls (sections 28, 28A, 29 and 31 (IFTR))
- Record keeping controls and ongoing staff training/awareness.

Where applicable, the RMCP must also indicate the sub-sections that are not applicable to the institution and reasons why they are not applicable.

Risk-based approach

A risk-based approach requires business to have an entity-wide understanding of the ML, TF and PF risks to which they are exposed. This approach allows businesses to allocate resources strategically towards higher-risk areas, while implementing streamlined procedures for lower-risk activities, thereby fostering efficient, effective, and adaptable risk management. The institution will be able to apply effective and proportionate ML, TF and PF controls. Risk assessment and identification are the basis of the accountable institution's RMCP. Revised Guidance Note 7A (2025) sets out the current principles for adopting a risk-based approach, including roles of the highest authority, documentation standards and proportionality in controls.

An institution will not be able to draft an effective RMCP without conducting a risk assessment. Therefore, an RMCP that is generic or presented as a template cannot be recognised and accepted. Instead, it will be regarded as a document that fails to satisfy the technical requirements outlined in section 42 of the FIC Act. Chapter 1 of the Revised Guidance Note 7A discusses in detail the principles that apply for the implementation of a risk-based approach.

Risk assessment

The institution needs to evaluate the risks associated with its clients, geographical location, products, services, delivery channels, and any other relevant factors. As an example, the entity-wide risk assessment of a law firm that provides only conveyancing services, would be different to that of a law firm that offers civil litigation. The monitoring,

mitigation and management controls that must be applied to the different risk ratings must be clearly noted. The steps that must be taken after having assessed the risks must also be indicated.

Client factors that may indicate heightened ML/TF/PF risk include, but are not limited to: clients who are DPIPs or FPPOs (and their immediate family members/known close associates), complex or opaque ownership structures, and clients linked to higher-risk jurisdictions or sanctions exposure.

Below are questions that may help in identifying heightened ML, TF and PF risk factors relating to products and services. This list is not prescriptive or exhaustive.

- To what extent does the product provide anonymity to the client
- Does the product enable third parties who are not known to the institution to make use of it
- Does the product allow for third party payments
- Is another accountable institution involved in the usage of the product
- Can the product be funded with cash or must it be funded only by way of a transfer to or from another financial institution
- How easily and quickly can funds be converted to cash
- Does the product facilitate the cross-border transfer of funds
- Is the offering of the product subject to regulatory approval and/or reporting
- What do the product enablement processes entail and to what extent do they include additional checks such as credit approvals, disclosure of information, legal agreements, licensing, regulatory approvals, registration, involvement of legal professionals, etc.
- To what extent is the usage of the product subject to parameters set by the institution such as value limits, duration limits, transaction limits, and to what extent is the usage of the product subject to penalties when certain conditions are not adhered to.

The RMCP document must provide for the documenting of decisions taken when dealing with the different levels of ML, TF and PF risks.

Submission of an RMCP

It is imperative for institutions to ensure that they have an effective, actionable RMCP which must be made available to the FIC in terms of section 42(4)(a). The RMCP must be submitted via the FIC's registration and reporting platform, and the name and file

must be in the prescribed format. Failure to develop an RMCP and/or make available a copy to the FIC may result in enforcement action being taken against the institution.

For compliance information and guidance, refer to the FIC website (www.fic.gov.za). The FIC's compliance contact centre can be reached on +27 12 641 6000 or log an online compliance query by clicking on: https://www.fic.gov.za/compliance-queries/