AML Compliance Checklist

A Practical Guide for South African Businesses

Anti-Money Laundering (AML) compliance is not optional in South Africa. The Financial Intelligence Centre Act (FICA), as amended by the FIC Amendment Act, imposes strict obligations on accountable and reporting institutions. Non-compliance can result in criminal prosecution, administrative sanctions, and reputational damage.

Use this checklist to assess your organisation's AML readiness across the key compliance areas. Tick each item as you verify it is in place, and identify gaps that need immediate attention.

Who should use this checklist: Banks, insurance companies, estate agents, attorneys, accountants, motor vehicle dealers, crypto asset service providers, high-value goods dealers, and any business designated as an accountable or reporting institution under FICA.

1. Risk Management and Compliance Programme (RMCP)

- ☐ A Board-approved Risk Management and Compliance Programme (RMCP) is in place and documented
- ☐ The RMCP identifies and assesses money laundering (ML) and terrorist financing (TF) risks specific to your business
- ☐ The RMCP has been updated within the last 12 months to reflect regulatory or business changes
- ☐ Risk mitigation measures are defined for each identified risk category (customers, products, geographies, channels)
- ☐ The RMCP includes procedures for enhanced due diligence (EDD) for high-risk clients
- ☐ An independent review or audit of the RMCP has been conducted within the prescribed period

2. Customer Due Diligence (CDD)

- ☐ All new clients are identified and verified before establishing a business relationship
- ☐ Acceptable identification documents are defined and consistently collected (ID, passport, company registration)
- ☐ Beneficial ownership is identified and verified for all legal entities and trusts
- ☐ Source of funds and source of wealth are established for higher-risk clients
- ☐ Simplified due diligence criteria are defined and applied only where risk is demonstrably low

- ☐ Enhanced due diligence procedures are applied for Politically Exposed Persons (PEPs), high-risk jurisdictions, and complex structures
- ☐ Ongoing due diligence is performed: client information is kept up to date and transactions are monitored
- ☐ Procedures exist for handling clients who refuse or fail to provide required CDD information

3. Record-Keeping

- ☐ All CDD records (identification, verification, and transaction records) are retained for at least five years after the relationship ends
- ☐ Records of all reportable transactions (STRs, CTRs, TPRs) are maintained and accessible
- ☐ Record-keeping procedures comply with FICA Section 22 to 27 requirements
- ☐ Electronic record-keeping systems are secure, backed up, and allow timely retrieval for regulatory requests
- ☐ A record retention and destruction policy is documented and followed

4. Reporting Obligations

- ☐ Suspicious Transaction Reports (STRs) are filed with the FIC promptly upon forming a suspicion (Section 29)
- ☐ Cash Threshold Reports (CTRs) are filed for all cash transactions of R24,999.99 or above (Section 28)
- ☐ Terrorist Property Reports (TPRs) are filed where applicable (Section 28A)
- ☐ Staff know how to escalate potential suspicious activity internally before filing
- ☐ A log of all reports submitted to the FIC is maintained with dates, reference numbers, and outcomes
- ☐ The goAML system is registered and operational for electronic filing

5. Compliance Officer and Governance

- ■ A suitably qualified and experienced Compliance Officer has been appointed and registered with the FIC
- ■ The Compliance Officer has direct access to the Board or senior management
- ■ The Compliance Officer's responsibilities are clearly defined and documented
- ■ There is a designated deputy or alternate Compliance Officer in case of absence
- ■ The Compliance Officer reports regularly to the Board on AML/CFT matters
- ■ Board members and senior management understand their personal liability for non-compliance

6. Training and Awareness

- ■ All employees receive AML/CFT training within their first 30 days and at least annually thereafter
- ■ Training covers: identifying suspicious transactions, CDD procedures, reporting obligations, and internal escalation
- ■

9. FIC Inspections and Regulatory Readiness

- ■ All compliance documentation is organised and readily available for FIC inspections
- ■ Previous FIC inspection findings (if any) have been fully remediated
- ■ A self-assessment against FIC Guidance Notes and Directives has been completed in the last 12 months
- ■ Correspondence with the FIC and supervisory bodies is logged and responded to within required timeframes
- ■ A designated point of contact for regulatory enquiries is identified and known to all relevant staff

Your Compliance Score

Count the number of items you ticked across all nine sections and use the guide below to assess your organisation's AML compliance posture.

Score Range	Rating	Recommended Action
47 - 52	Excellent	Maintain your programme. Schedule an annual review to stay current.
38 - 46	Good	Address identified gaps within 60 days. Consider an external compliance audit.
25 - 37	Needs Improvement	Significant gaps exist. Engage specialist AML counsel to remediate urgently.
Below 25	Critical	Your organisation is at serious risk of regulatory action. Seek immediate legal assistance.

Range
Ran-48 384 S Td ge