South African Reserve Bank
Prudential Authority

Anti-money laundering, counter-financing of terrorism and counter-proliferation financing (AML/CFT/CPF) awareness communiqué

AML/CFT/CPF Communication 1 of 2023

Introduction

The Prudential Authority (PA) is the designated supervisory body[1] responsible for ensuring that banks, mutual banks, co-operative banks and life insurers (hereinafter referred to as accountable institutions (AIs)) comply with the provisions of the Financial Intelligence Centre Act 38 of 2001 (FIC Act), as amended.

Purpose of this communiqué

The purpose of this communiqué is to update AIs on the key observations (deficiencies) identified by the PA through its AML/CFT/CPF supervision of AIs.

The PA will also periodically update the key observations (deficiencies) emanating from such supervision. These communiqués will be published on the South African Reserve Bank's website under the heading: 'Prudential Regulation: AML/CFT/CPF'.

Prudential Authority expectations

The PA expects AIs to:

- take note of the deficiencies; and
- scrutinise their AML/CFT/CPF frameworks with a view of enhancing their risk management and compliance programmes where deemed necessary.

Key deficiencies identified through supervision

Annexure A attached hereto provides details of the deficiencies identified for the period 1 April 2019 to 31 March 2023, together with guidance on the PA's expectations[2] on how AIs should implement effective controls.

Fundi Tshazibana

Fundi Tshazibana
Chief Executive Officer

Date: 10/11/23

Encl. 1

[1] Schedule 2 of Financial Intelligence Centre Act 38 of 2001, as amended.
[2] The aforementioned does not in any way replace the remedial actions or directives imposed on accountable institutions by the PA in terms of the FIC Act, neither does it replace any guidance issued by the FIC.

Observations arising from AML/CFT/CPF supervision by the Prudential Authority

Period of review: 1 April 2019 to 31 March 2023 (48 months)

References to 'section(s)' and 'regulation(s)' in this document invariably refer to section(s) and regulation(s) of the Financial Intelligence Centre Act 38 of 2001, as amended (FIC Act) and the Money Laundering and Terrorist Financing Control Regulations (Regulations).

	Key deficiencies observed	Comments and the PA's expectations
1.	**Risk management and compliance programme (RMCP)**	
a.	**Business risk assessment (BRA)** • An accountable institution (AI) had not documented the methodology followed to assess the money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks inherent to its business operations. • The BRA was conducted at a general level, without delving into specific details concerning ML/TF/PF risk factors and did not adequately reflect the AI's understanding of ML/TF/PF risks specific to its business. • The BRA did not address/cover PF risk. • The outcome of the BRA was not referred to any internal governance forum(s) for deliberation and approval.	All AIs should take into account guidance issued by the FIC. Additionally, guidance issued to banks on business risk assessments (Guidance Note G6/2022 dated 15 June 2022, issued by the Prudential Authority (PA), in terms of section 6(5) of the Banks Act 94 of 1990.) should be considered.

	Key deficiencies observed	Comments and the PA's expectations
	• The BRAs in respect of a foreign branch(es) operating in South Africa did not address ML/TF/PF risk from a South African perspective (thus the BRA of the branch only reflected the international group's global understanding of ML/TF/PF risk). • The RMCP did not indicate the rationale for the inclusion of certain risk factors and the assigned risk weightings were not documented in the RMCP/BRA.	
b.	**FIC Act obligations/related policies and procedures** • The RMCP did not sufficiently address all obligations prescribed in the FIC Act; • The RMCP did not include a description of the board of directors' or senior management's accountability (responsibilities) to assist with ensuring compliance with the FIC Act. • The AI could not evidence that the board of directors/senior management had approved the RMCP. • The AI could not evidence the periodic review of the RMCP (thus the RMCP did not reflect updates confirming that emerging ML/TF/PF risks or new guidance issued by regulators had been taken into account.	Section 42 of the FIC Act places an obligation on AIs to develop, document, maintain and implement an RMCP. An AI's ability to apply a risk-based approach (RBA) effectively is largely dependent on the quality of its RMCP and the business risk assessment forms a key component of the RMCP as it will determine the controls required to mitigate and manage the ML/TF/PF risk to which the bank/LI is exposed to.

	Key deficiencies observed	Comments and the PA's expectations
	• The AI had not developed and/or documented step-by-step procedures for all/certain of its FIC Act obligations. • Relevant AML/CFT policies and step-by-step procedures were not referenced in the RMCP, for example: − sanctions policy; and − human resources policy (consequences for non-compliance with the FIC Act/other legislation).	
c.	**ML/TF/PF risk-scoring model/matrix (RSM)** • The AI had not risk-scored its clients (or all its clients) for ML/TF/PF purposes (e.g. high, medium or low risk). • The RSM (methodology) used by the AI was ineffective/too simplistic, for example: − not all products offered by the AI were covered; − geographic/delivery channel risk factors were not considered; − no provision was made for an adverse media/ manual override of a risk score; − no provision was made for factors such as intelligence reports filed with the FIC; and − the rationale and the algorithm used in determining the ML/TF/PF customer risk score were not clearly articulated. • The RSM had not been approved or was not periodically reviewed.	An AI's RSM must: • be comprehensive and cover all risk factors; • be commensurate with the assessed ML/TF/PF risk; • be approved by appropriate governance structure(s); • clearly document the rationale relating to the risk scores assigned to the risk factors on its RMS model; and • be reviewed periodically.

	Key deficiencies observed	Comments and the PA's expectations
d.	**Risk-based approach (RBA)** • There was a mismatch between the number of high-risk clients reflected on the active client list versus the number of high-risk clients reflected on the AI's enhanced due diligence (EDD) register/list of high-risk clients. • Trade finance transactions (cross-border payments) had not been processed in accordance with the payment requirements stipulated in the AI's RMCP. • The use of unstructured supplementary service (USSD) technology (found in non-smart mobile phones) to onboard clients did not enable the AI to **verify** the identity of the client, resulting in the AI being non-compliant with section 21(1) of the FIC Act.	An AI must ensure that its risk-based approach is implemented correctly, including: • correct categorisation of clients according to ML/TF/PF risk; • appropriate alignment of procedures and the approved RMCP; • alignment with the FIC Act principles on EDD, ongoing due diligence (ODD) and customer due diligence (CDD); and • ensuring that the RBA improves the efficacy of measures to counter ML and TF while promoting financial inclusion without undermining AML/CFT objectives.
2.	**Customer due diligence**	
a.	EDD reviews pertaining to high-risk customer relationships did not adhere to the EDD requirements documented in the AI's RMCP. Deficiencies identified included that: • EDD reviews were not dated; • EDD reviews lacked evidence of supporting documents (e.g. outcomes of adverse media searches and client transaction account searches); • EDD reviews lacked evidence of the outcome of the review of a customer's account statements/activity); • EDD reviews did not reflect a recommendation by the EDD reviewer regarding whether the business	• AIs must implement adequate controls to ensure that: − EDD reviews are duly completed and contain all supporting documentation as prescribed in the AI's RMCP; and − controls are implemented to ensure that EDD reviews are completed within the timelines stipulated in the AI's RMCP. • Compliance units must conduct periodic reviews to ensure that business units comply with prescribed EDD processes.

	Key deficiencies observed	Comments and the PA's expectations
	relationship should be retained or exited, or if the ML/TF risk score should be adjusted; • EDD reviews had not been completed within the timelines prescribed in the AI's RMCP; and • EDD reviews were not approved/signed off by senior management.	
b.	Ongoing due diligence (ODD) (section 21C) review of existing customer relationships: • had not been conducted and/or completed in accordance with the requirements prescribed in the AI's RMCP; and • lacked information pertaining to: − the nature of the business relationship; − the intended purpose of the business relationship; and − the source of the funds.	• Business units of AIs must implement adequate controls to ensure that: − ODD reviews are duly completed and contain all supporting documentation as prescribed in the AI's RMCP; − The timelines for review align to the risk profile of the client (e.g. higher risk clients require more frequent reviews); − controls are implemented to ensure that ODD reviews are completed within the timelines stipulated in the AI's RMCP. • Furthermore, compliance units must conduct periodic reviews to ensure that business units comply with prescribed ODD processes.
c.	The AI had not implemented a process/system to identify foreign politically exposed persons and domestic politically exposed persons as well as prominent influential persons (hereinafter collectively referred to as PEPs) [sections 21F, 21G]. The PEP screening system used by the AI was ineffective (e.g. it did not generate alerts for altered/manipulated data of sanctioned persons (e.g. names, date of birth and identity number, resulting in fuzzy logic).	An AI must ensure that controls implemented/systems deployed to detect PEPs are effective and cater for: • exact matches; and • fuzzy logic scenarios.

	Key deficiencies observed	Comments and the PA's expectations
d.	Beneficial owners in respect of legal persons had not been duly identified (section 21B).	An AI must ensure that its customer onboarding practices enable it to: • duly identify beneficial owners of legal persons and trusts; and • demonstrate to the supervisor the methodology/process followed to identify the beneficial owner, over and above legal ownership and inclusive of control through other means.
3	**Record keeping**	
a.	Records of customer relationships and transactions had not been kept for a period of five years after the termination of the relationship. The AI had not notified the FIC that a third party was keeping records on its behalf (section 24(3)). Records in respect of suspicious and unusual transaction reports (STR) and suspicious activity reports (SARs) were not duly kept.	An AI must ensure that it implements adequate systems and controls to ensure that it complies with record-keeping requirements prescribed in sections 22 to 24 of the FIC Act.
4.	**Filing of intelligence reports with the FIC and controls implemented to meet legislative obligations**	
4.1	**Cash threshold reporting**	
a.	Cash threshold reports (CTRs) were filed with the FIC beyond the prescribed period of three business days. The AI failed to identify and report all reportable cash transactions to the FIC as CTRs.	An AI must ensure that it implements adequate systems and controls to ensure that it files CTRs with the FIC in accordance with section 28, read with regulation 24(4), of the FIC Act.
4.2	**Terrorist property reporting**	

	Key deficiencies observed	Comments and the PA's expectations
a.	The AI could not produce evidence (documented or on a screening system) that at onboarding it had screened: • prospective/new customers; and/or • parties related to a customer (e.g. account signatories, ultimate beneficial owners, trustees, trust beneficiaries and donors).	An AI must be able to evidence that it had screened (manually or via an automated solution) its customers and parties related to a customer: • prior to entering into a business relationship; and • on a periodic basis thereafter (e.g. daily, weekly, monthly) in accordance with the screening requirements/policies documented in its RMCP.
b.	The AI could not explain which sanctions lists (other than United Nations Security Council Resolution 1267) were deployed in its sanctions-screening system or explain the rationale for including or excluding certain lists.	An AI must document in its RMCP, or screening policies referenced in its RMCP, details of: • all the sanctions source lists (public and any internally generated lists, if applicable) it had opted to screen its customers against in accordance with its risk appetite; and • the reason(s) for incorporating the particular lists in its sanctions-screening programme.
c.	The sanctions-screening system deployed was not optimally configured (e.g. screening systems did not generate alerts for sanctioned persons where the PA had changed (manipulated) the names, resulting in fuzzy logic).	An AI must review the effectiveness of its sanctions-screening system(s)' algorithmic parameters on an ongoing basis to ensure that it is in a position to identify sanctioned persons commensurate with its risk appetite and tolerance levels.

	Key deficiencies observed	Comments and the PA's expectations
4.3	**Suspicious and unusual transaction reports/ suspicious activity reporting**	
	Automated transaction monitoring system (ATMS) • ATMS rules deployed were insufficient and/or ineffective (i.e. the rules did not enable the AI to detect suspicious and unusual transactions). • ATMS rules deployed were not periodically reviewed. • ATMS rules were not subjected to any internal audit/ third-party review. • ATMS rules deployed or changes made to the rules over time had not been approved by an appropriate governance forum. • ATMS alerts were not attended to within 48 hours. ATMS alert investigations • Outcomes of alert investigations were not duly documented (i.e. the same reasons were provided/ used for multiple alerts). Other • STRs/SARs were not filed with the FIC as soon as possible. • SARs/STRs were not filed with the FIC within the prescribed reporting period.	AIs that have opted to deploy an ATMS to detect suspicious and unusual transactions must ensure that it adheres to the requirements prescribed in FIC Directive 5 dated 29 March 2019. Furthermore, an AI must ensure that STRs/SARs are filed with the FIC as soon as possible but not later than 15 business days after the institution becomes aware, or suspicion is raised regarding an activity or transaction.
5	**Training (Section 43)**	
a.	The training material did not address all FIC Act obligations and/or requirements stipulated in the AI's RMCP.	The FIC Act requires that an AI provides **ongoing** training to its employees to enable them to comply with the provisions of the FIC Act and its RMCP which are applicable to them.

	Key deficiencies observed	Comments and the PA's expectations
		Therefore, an AI must provide adequate training on ML/TF/PF to ensure that employees are aware of, and understand, their legal and regulatory responsibilities as well as their role in handling criminal property and ML/TF/PF risk management.
b.	Training material was not periodically reviewed and/or updated.	An AI must ensure that its training material is periodically updated to reflect the: • requirements with current AML/CFT/CPF legislation; • guidance issued by supervisors (where applicable to the AI); and • latest ML/TF/PF trends and typologies.
c.	The AI did not provide specialised training to staff tasked to perform certain obligations under the FIC Act.	Employees involved in certain key obligations under the FIC Act must be provided with intensive (specialised) training on the provisions of the FIC Act (e.g. the investigation of suspicious and unusual transaction alerts, the investigation of sanction-screening system alerts, dealing with trade finance clients and the processing of related transactions).
d.	Induction and/or refresher AML/CFT/CPF training was not provided within the timelines prescribed in the AI's RMCP.	Training at onboarding and on an ongoing basis should be performed, and this must be reflected in the RMCP, including the frequency of training and whether specialised or general training is required. Training must take place as per the documented RMCP and must be tailored to the needs of the AI.
e.	The AI's board of directors and/or senior management had not received any AML/CFT training.	• Section 42A(1) of the FIC Act states that the board of directors of an AI which is a legal person with a board of directors, or the senior management of an AI without a board of directors, must ensure compliance by the AI and its employees with the provisions of the FIC Act and its RMCP.

	Key deficiencies observed	Comments and the PA's expectations
		• In order for the members of the board of directors to duly execute their responsibilities under the FIC Act, they need to be trained on the requirements of the FIC Act. • FIC Act training material should be customised to train the board of directors. The AI must keep a register/record of training provided to board members.
f.	There was insufficient follow-up by the AI (either by the Compliance Unit or the Human Resources Department) pertaining to employees who had failed knowledge assessments.	Some AIs have implemented online interventions to train employees. In some instances, it was observed that the training platforms were not duly monitored to ensure that employees who had failed the training are subjected to retests and successful completion.
g.	Training registers did not contain certain data (e.g. dates, manual or digital signatures).	Data missing from registers included employee signatures (where face-to face training is provided), the date on which the training intervention took place and unreadable text (names of employees) recorded in the registers. An AI must ensure that training registers can be reconciled with lists of active employees and that proper training records are kept at all times.
5.	**Governance**	
a.	The AI's Compliance Unit was not adequately resourced to ensure compliance with the FIC Act.	This matter is raised when it is clear that the AI has, over time, failed to meet its obligations under the FIC Act, for example: • experiencing backlogs in processing transaction monitoring system alerts and sanctions-screening system alerts within the timelines prescribed in the AI's RMCP; • experiencing backlogs in conducting ODD and EDD reviews on client relationships in accordance with the AI's RMCP; • not filing intelligence reports within the timelines prescribed in the FIC Act; and

	Key deficiencies observed	Comments and the PA's expectations
		• inadequate documenting of the outcome of alert investigations (this excludes a lack of proper specialised training).