P O Box 427 Pretoria 0001 South Africa
370 Helen Joseph Street Pretoria 0002
+27 12 313 3911 / 0861 12 7272
www.resbank.co.za

South African Reserve Bank
Prudential Authority

Ref.: 15/8/1/2

G10/2022

To: All banks, branches of foreign institutions, controlling companies, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Supervisory guidelines for matters related to the prevention of banks or controlling companies being used for any money laundering, terrorist financing or other unlawful activity

Executive summary

The purpose of this Guidance Note is to inform banks and controlling companies of practices related to the effective implementation of adequate anti-money laundering and counter-financing of terrorism (AML/CFT) controls in relation to crypto assets (CAs[1]) and crypto asset service providers (CASPs).

Regulation 36 (17) of the Regulations relating to Banks (the Regulations) requires that every bank and every controlling company shall have in place board approved policies and comprehensive risk-management processes and procedures, which policies, processes and procedures include comprehensive and robust know-your-customer standards that inter alia include robust customer identification, verification and acceptance requirements throughout the banking group, contribute to the safety and soundness of the reporting bank or controlling company, and prevent the bank or controlling company from being used for any money laundering or other unlawful activity.

Further to this, Regulations 36(17)(b)(ii), 47 and 50 impose high-level requirements related to banks' corporate governance, risk management, internal controls, policies, processes, and procedures to ensure ongoing compliance with best practices related to matters such as AML/CFT, reportable offences and to guard against the bank being used for purposes of financial crimes, such as financing of terrorist activities and money laundering. Regulation 38(4) of the Regulations provides that when the Prudential Authority (PA) is of the opinion that a bank's policies, processes, and procedures relating to its risk assessment are inadequate; or its internal control systems are inadequate; etc., the PA may, among other things, require the bank to strengthen its risk management policies, processes or procedures; or to strengthen the bank's internal control systems.

1 Financial Action Task Force terminology refers to virtual assets and virtual asset service providers.

1. Introduction

1.1. The Financial Action Task Force (FATF) Guidance on the risk-based approach in the banking sector[2] clearly stipulates that the risk assessment underpins the bank's risk-based approach. It must enable the bank to understand how, and to what extent, it is vulnerable to money laundering, terrorist financing and proliferation financing (ML/TF/PF). It necessitates an evidence-based and informed categorisation of risk at various levels, which will help banks determine the level of AML/CFT and counter-proliferation financing (CPF) resources necessary to mitigate that risk. All relevant information must always be properly documented, maintained and communicated to relevant personnel within the bank, controlling company and other relevant group entities.

1.2. FATF Recommendation 15 of the FATF Recommendations[3] specifically mentions that:

> Financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.
>
> In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

1.3. The Basel Committee on Banking Supervision Guidelines (BCBS guidelines) on the sound management of risks relating to ML/TF highlighted that not all digital currencies are widely used or accepted, due to absence of a trusted third party, which impacts the safety and efficiency of payment, clearing, settlement and related arrangements in support of financial stability. The degree of anonymity impacts on the ability to evidence implementation of AML/CFT requirements in relation to digital currency transactions. It was noted that CAs and related services have the potential to raise financial stability concerns and increase risk faced by banks.

1.4. The requirements for preventive measures are dealt with in the Financial Intelligence Centre Act 28 of 2001 (FIC Act) and requires the application of a risk-based approach when dealing with matters concerning customer due diligence.

1.5. Section 42 of the FIC Act requires banks to develop, document, maintain and implement a programme for AML/CFT which must enable the bank to identify, assess, monitor, mitigate and manage the risk of products or services which are susceptible to facilitate ML/TF activities and/or risks.

---

2 https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

3 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

1.6. The PA acknowledges that in the context of banks, holding companies, controlling companies and/or banking groups, detailed and thorough business ML/TF/PF risk assessments are imperative for the demonstration of thorough ML/TF/PF risk appreciation specific to all relevant group entities.

1.7. The business risk assessment must be conducted systematically while including a sufficient range of inherent risk factors to identify and reflect an in depth understanding of ML/TF/PF risk at an institutional level.

1.8. Regulation 38(4) of the Regulations states, among others, when the PA is of the opinion that a bank's policies, processes and procedures relating to its risk assessment or internal control systems are inadequate, the PA may require the bank, among others:

1.8.1. to strengthen the bank's risk management policies, processes or procedures; or
1.8.2. to strengthen the bank's internal control systems.

1.9. The PA is aware that certain banks in South Africa have previously opted to terminate the bank/customer relationship with CASPs or discontinued banking services to CASPs. This approach of banks to CASPs may be premised on various reasons, including the uncertainty in relation to the ML/TF/PF risk that CASPs present or the lack of formal regulatory requirements applicable to CASPs. Underlying the banks' approach to providing banking services to CASPs is the perception that CASPs' clients generally pose a higher risk of using their CASP accounts to launder money, violate sanctions and support other illicit activities.

1.10. Risk assessment does not necessarily imply that institutions should seek to avoid risk entirely (also referred to as de-risking), for example, through wholesale termination of client relationships which may include CASPs. De-risking may pose a threat to financial integrity in general and to the application of a risk-based approach, specifically, as it could potentially create opacity in the affected persons' or entities' financial conduct, and it eliminates the possibility to treat ML/TF/PF risks.

1.11. It is thus prudent for banks to be able to risk categorise CA/CASP related clients through conducting a risk assessment which will assist banks in determining the appropriate level of ML/TF/PF risk management measures necessary, as opposed to total avoidance, in line with the application of a risk-based approach.

1.12. If the risk posed by a particular business or customer is too great to manage successfully, the decision to de-risk should only be made after careful due diligence[4] and consideration[5].

---

4 https://www.acamstoday.org/de-risking-does-one-bad-apple-spoil-the-bunch/.

5 https://www.fsca.co.za/Notices/FSCA%20Conduct%20Standard%203%20of%202020%20(BANKS)-Banks.zip.

1.13. This Guidance Note seeks to provide guidelines on certain aspects linked to the treatment of CASPs and CAs based on the application of a thorough risk-based approach.

2. Definitions

2.1. **Crypto Asset:** A digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. CAs do not include digital representations of fiat currencies, securities, and other financial assets that are already covered in FATF Recommendation 15.[6]

2.2. **Crypto Asset Service Provider:** any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conduct one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between CAs and fiat currencies;

ii. exchange between one or more forms of CAs;

iii. transfer of CAs;

iv. safekeeping and/or administration of CAs or instruments enabling control over CAs; and

v. participation in and provision of financial services related to an issuer's offer and/or sale of a CA[7].

2.3. Within South Africa, the following activities were identified as being performed by CASPs as per the Crypto Asset Regulatory Working Group's Position Paper on CAs[8]:

Table 1: Activities performed by CASPs

No.	CASP	Services offered
1	CASP (or any other entity facilitating or providing the mentioned services (i.e., CA automated teller machines, CA kiosks etc.)	These are CASPs providing the following: • intermediary services for the buying and selling of CAs; • the trading, conversion or exchange of fiat currency or other value into CAs; • the trading, conversion or exchange of CAs into fiat currency or other value; • the trading, conversion or exchange of CAs into other CAs; • remittance services using CAs as a means of facilitating credit transfers

6 FATF Guidance for a risk-based approach to virtual assets and virtual asset service providers (updated October 2021).
7 As above.
8 Intergovernmental Fintech Working Group Crypto Assets Regulatory Working Group Position Paper on Crypto Assets Available at: https://www.ifwg.co.za/wp-content/uploads/IFWG_CAR_WG_Position_Paper_on_crypto_assets.pdf.

No.	CASP	Services offered
		(remitter or value transfer provider); and • providing advice in relation to CAs.
2	CA vending machine operator	• These entities provide intermediary services for the buying and selling of CAs (including any of the above-mentioned services).
3	CA token issuer/distributor	These are CASPs conducting token issuances and distributions, including: • initial coin offerings;[9] • the issuance of stablecoins; • the issuance of global stablecoins; • the distribution of stablecoins; and • the participation in, and provision of, financial services related to an issuer's offer or sale or distributing of CAs.
4	CA fund or derivative service provider	These entities offer investment funds or derivative products with CAs as the underlying asset.
5	CA digital wallet provider (custodial wallet providers only[10])	These entities offer a software program with the ability to store private and public keys that are used to interact with various digital protocols which enable the user to send and receive CAs, with the additional ability to monitor balances and execute control over the customers' CAs.
6	CA safe custody service provider (custodial service)	These entities safeguard, store, hold or maintain custody of CAs belonging to another party.

3. Application of a risk-based approach: Identification and assessment of risks relative to CAs and CASPs

3.1. A comprehensive ML/TF/PF risk assessment will enable banks to clearly comprehend the direct and/or indirect exposure to any form of CASPs, CAs and/or related activities.

9 From a FATF point of view, the expectation is not that the issuer of tokens in an ICO should be an obliged entity, but anybody who provides financial services in respect of an ICO should be. The analogy to this is where a company is formed and has an initial public share offer. The company issuing the shares is not an obliged entity, but the bank that underwrites the offering or offers credit for people who take up the public offer, is an obliged entity. However, all other requirements imposed on CASPs as detailed in this document will apply to crypto asset token issuers.

10 Non-custodial wallets are excluded as these types of wallets lack the ability to execute control over crypto assets.

3.2. To effectively implement AML/CFT monitoring, mitigating, and managing controls, banks should evidence an understanding of what elements are driving or reducing ML/TF/PF risk within CASPs and CAs in the context of their institutions, e.g., giving regard to the type of clients banked, the transactional activity, cross border flow of funds and association with crypto related activity by a particular client.

3.3. Certain products or services offered may have a higher propensity for utilisation by CASPs or customers engaging in CASP activity.

3.4. Banks will only be able to identify the appropriate level of controls and systems required to mitigate the degree of risk posed after a comprehensive ML/TF/PF risk assessment in respect of CASPs and CAs has been conducted.

3.5. As part of the risk management and compliance programme of the bank, documented policies, procedures and internal controls are required to be tailored and cater for the varying levels of risk that CASPs and CAs, as well as threats by customers engaging in such activity, may pose.

3.6. The implemented controls must be robust and flexible to adapt to changes encountered regarding technology development and the appreciation of ML/TF/PF risk should inter alia be based on the entity's business model, size, the nature of transactions etc.

3.7. The requisite policies and procedures to give effect to the aforementioned should be documented and updated as often as may be required.

3.8. The enquiry at on-boarding should be sufficient to enable the bank to establish a risk profile in respect of the CASP as a client, and subsequently implement and apply due diligence measures commensurate with the degree of risk posed by such client. This enables a bank to effectively manage the degree of risk posed by a client. Banks should collect sufficient information to understand the nature of the CASP's business and its risk profile. It is thus prudent that the risk assessment reflects consideration of all relevant risk factors, including but not limited to the types of services, products, or transactions involved; customer risk; geographical factors; and the type(s) of CA exchanged.

3.9. When a bank seeks to establish and maintain a business relationship or conclude a single transaction with a CASP, it should ascertain as part of its due diligence if the CASP client has documented and implemented appropriate ML/TF/PF risk management policies, procedures, systems, and controls etc. that it follows in respect of its own activities and business offerings.

3.10. Where higher risks present themselves via client relationships or at onboarding, enhanced due diligence should be undertaken.

3.11. Banks should also assess AML/CFT/CPF controls of the CASP to be aligned to new technical developments aligned to CASPs' character. A "one-size-fits-all" approach in dealing with CASPs/CAs from a ML/TF/PF risk perspective may signify inadequate risk understanding and risk management, as business models may widely differ, and this goes against the spirit and practice of a risk-based approach.

3.12. As the risks associated with CASPs and CAs are constantly changing, it is imperative that banks conduct regular risk assessments and amend their risk profiles and risk management programmes in accordance with the emerging risks insofar as their entities may be impacted.

3.13. Banks should ensure that they have the relevant and requisite technical expertise to adequately assess the risks stemming from CASPs and CAs.

4. Monitoring of client relationships

4.1. It is essential that banks understand the transactional activity of their clients and whether or not such activity is in line with the initial profile held in respect of the client, as criminals may exploit conduits and customers to move large sums of money which form the proceeds of crime to purchase CAs. Any suspicious or unusual activity[11] must be reported to the Financial Intelligence Centre (FIC) in terms of section 29 of the FIC Act.

4.2. When banks become aware of any terrorist property being introduced to its business linked directly or indirectly to CASPs or CAs, it must report same to the FIC in terms of section 28A of the FIC Act. Banks must ensure they employ appropriate detection and monitoring mechanisms to mitigate this risk.

4.3. Banks may act as a conduit for funds linked to CASP activity and may play a role in customers wishing to purchase CAs or receive pay-outs for the sale of CAs via fiat currency into their bank accounts. Banks must ensure that they maintain adequate records in respect of all customer transactions, including fiat-to-fiat (i.e., from CASP customer's bank account to the CASP bank account and vice versa), fiat-to-crypto and crypto-to-fiat transactions for a minimum period of five years or five years from the date of submission of a suspicious or unusual transaction report to the FIC.

4.4. Ongoing due diligence should be performed in respect of all customers and adequate transaction monitoring measures implemented to detect the aforementioned suspicious or unusual activity.

[11] See the FATF report on virtual assets red flag indicators of terrorist financing. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

5. Acknowledgment of receipt

5.1. Kindly ensure that a copy of this guidance note is made available to your institution's independent auditors. The attached acknowledgment of receipt duly completed and signed by both the Chief Executive Officer of the institution and the said auditors should be returned to the PA at the earliest convenience of the aforementioned signatories.

Fundi Tshazibana

Fundi Tshazibana
Chief Executive Officer

Date: 15 August 2022

The previous guidance note issued was Guidance Note 9/2022, dated 29 July 2022.