BANK OF BOTSWANA

BUSINESS CONDUCT AND REGULATORY COMPLIANCE DEPARTMENT

GUIDELINE ON SIMPLIFIED DUE DILIGENCE MEASURES

Issue Date: 24 February 2026

TABLE OF CONTENTS

Authority, Scope and Purpose

(a) Authority

1.1 This Guideline is issued by the Bank of Botswana (Bank), pursuant to its authority provided for in Section 49(1)(c) of the Financial Intelligence Act, 2022 (Cap. 08:07), which empowers the Bank to issue instructions or guidelines to help financial institutions comply with the Act.

(b) Purpose of the Guideline

1.2 The purpose of this Guideline is to provide guidance for the implementation of Section 28 of the Financial Intelligence Act, 2022, which allows financial institutions to apply simplified customer due diligence measures to a particular business relationship or transaction where the risk of commission of a financial offence is assessed to be low.

1.3 This Guideline is not intended to supersede or replace any of the existing mandatory requirements on customer due diligence provided in Section 16 and 20 of the Financial Intelligence Act, 2022, the Financial Intelligence (Amendment) Act, 2025, and Rectification of the Laws (Financial Intelligence Act) (No.2) Order 2025, and only seeks to provide supplementary guidance on the circumstances and parameters under which simplified due diligence measures may be applied.

(c) Scope

1.4 This Guideline shall apply to the following financial institutions:

(a) Bank, banking group and deposit-taking institution licensed by the Bank under the Banking Act (Cap. 46:04) (Banking Act); or any other institution authorised to engage in banking under the powers conferred by any other legislation in accordance with Section 3(2) of the Banking Act, 2023;
(b) Bureau de change licenced under the Bureaux de Change Regulations, 2004; and
(c) Money or value transfer service provider and electronic payment service provider licensed under the Electronic Payment Services Regulations, 2019.

1.5 The Guideline specifies procedures and minimum conditions that must be fulfilled in order for a financial institution to apply simplified due diligence measures.

(d) Objectives

1.6 The promotion of formal financial systems and services is central to any effective and comprehensive anti-money laundering and counter the financing of terrorism and counter-proliferation financing (AML/CFT/CPF) regime. While robust safeguards are necessary, an overly conservative application of customer due diligence requirements can inadvertently exclude legitimate consumers and businesses from accessing formal financial services. Identifying and understanding the customer, including the parties who own or control them, not only fulfils legal and regulatory obligations, but also enables financial institutions to make informed risk-based decisions. However, the application of full customer due diligence measures may pose practical challenges for financial institutions serving low-income, marginalised, underserved, or informal

customer segments, thereby underscoring the need for proportionate and risk-based approaches such as simplified due diligence.

1.7 This Guideline therefore provides a general framework to support financial institutions in implementing AML/CFT/CPF measures that are consistent with Botswana's legal and regulatory requirements and broader national objectives, including advancing financial inclusion, promoting a cashless economy, and increasing the adoption and usage of digital financial services. It aims to foster a common understanding of the flexibility permitted under the Financial Intelligence Act, 2022, particularly the application of the risk-based approach, so as to balance financial integrity with accessibility. The Guideline also seeks to support more efficient know your customer (KYC) processes for both new and existing customers, enabling timely onboarding and ongoing verification while maintaining appropriate safeguards. Ultimately, it focuses on facilitating access to formal services for financially excluded and underserved groups and promoting the transition from cash-based activity towards secure, digital financial ecosystems.

(e) Responsibility

1.8 It shall be the responsibility of the senior management and Board of Directors of a financial institution to ensure that customer due diligence, including the application of simplified due diligence where a low risk is established in accordance with Section 28, is conducted in full compliance with the Financial Intelligence Act, 2022, the Financial Intelligence (Amendment) Act, 2025, Rectification of the Laws (Financial Intelligence Act) (No.2) Order 2025 and its Regulations (herein referred to as the FI Act).

2. Definition of Terms

2.1 Unless expressly defined in this Guideline or required otherwise by the context, the terms and expressions used shall bear the same meanings ascribed to them under the following respective Acts:

Act	Terms
Financial Intelligence Act, 2022, (FI Act), Financial Intelligence (Amendment) Act, 2025, Rectification of the Laws (Financial Intelligence Act) (No.2) Order 2025	(a) "beneficial owner" (b) "business relationship" (c) "customer" (d) "customer due diligence" (e) "enhanced due diligence" (f) "financial offence" (g) "high-risk business" (h) "high-risk jurisdiction" (i) "legal arrangement" (j) "national risk assessment" (k) "prominent influential person" (l) "simplified due diligence" (m) "suspicious transaction" (n) "transaction" (o) "ultimate effective control"

Financial Intelligence Regulations, 2022 (FI Regulations)	(a) "company" (b) "document" (c) "entity" (d) "identity card" (e) "manager"
Proceeds and Instruments of Crime Act, 2014	(a) "money laundering" (b) "property"
Counter-Terrorism Act, 2014	(a) "terrorist" (b) "terrorist group" (c) "act of terrorism"

2.2 For the purpose of this Guideline, operational definitions not already prescribed under the relevant Acts are set out below:

Term	**Definition**
"Bank"	Bank of Botswana, established under the Bank of Botswana Act (Cap. 55:01).
"complex ownership structure"	a multi-layered or opaque ownership or control arrangement involving multiple legal persons or legal arrangements, cross-border chains, nominees, bearer instruments, or other mechanisms that obscure, or could reasonably be expected to obscure, the identity of the natural person(s) who exercise ultimate effective control as defined under the FI Act.
"digital identity"	set of electronically captured and validated attributes that uniquely identify a person, created and used through official digital identification (ID) systems with identity assurance processes that are reliable, independent, and capable of strong verification, consistent with FATF's digital identity assurance levels.
"financial inclusion"	the provision of access to affordable, convenient, and appropriate financial services and products to all segments of society, to meet the needs of individuals and businesses who are traditionally underserved or excluded from the mainstream financial system.
"intermediary"	a person or entity that acts between the customer and the institution in establishing a business relationship or conducting transactions, including agents, brokers, introducers, or other third parties, whether regulated or unregulated.
"legal person"	any entity other than natural person, created by law and recognised as a legal entity having distinct identity, legal personality, duties and rights, that can establish a relationship with a financial institution or otherwise own property. Legal person can include companies, body

	corporate, foundations, partnerships, or associations and similar other entities that have legal personality.
"terrorist financing" (TF)	the financing of terrorist acts, and of terrorists and terrorist organisations, even in the absence of a link to a specific terrorist act or acts;
"proliferation financing" (PF)	the provision, acquisition, or movement of funds, assets, goods, or technology that contribute to the development, production, acquisition, or use of weapons of mass destruction, or that support persons or entities involved in such activities (proliferation financing).
"non-face-to-face"	activities (e.g. onboarding, transaction, or interaction) in which the customer is not physically present and identity is verified through remote or digital means.
"risk-based approach" (RBA)	the application of measures which commensurate with the level of ML/TF/PF risks identified, such that higher-risk situations attract more robust controls and lower-risk situations may be subject to simplified measures.
"verify"	establishing the truth of information received from the customer on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified.

3. Principles of Simplified Due Diligence

(a) What is Simplified Due Diligence

3.1 Simplified due diligence (SDD) is a form of customer due diligence (CDD) predicated on a risk-based approach (RBA), permitting institutions to apply less stringent measures for customers who pose a low risk of involvement in financial crimes such as money laundering/ terrorist financing/ proliferation financing (ML/TF/PF). SDD represents the lowest level of due diligence permissible and may involve simplifications to CDD measures such as:

(i) customer acceptance measures (i.e. identification and verification);
(ii) ongoing monitoring obligations; or
(iii) both, where appropriate.

3.2 As per Section 28 of the FI Act, SDD is permitted only where the risks of ML/TF/PF are assessed to be low, supported by:

(i) the institution's own ML/TF/PF risk assessments conducted pursuant to Section 13 of the FI Act;
(ii) any guidance notes issued by the Bank; and
(ii) the National Risk Assessment (NRA).

SDD measures must therefore be risk-based and proportionate, ensuring that the extent of due diligence measures corresponds to the level of risk identified.

3.3 SDD may be applied in the following circumstances, where the relationship, product, or transaction has been assessed to present low ML/TF/PF risk:

(i) when establishing a business relationship with a customer;
(ii) when conducting transactions or occasional transactions at or above the applicable thresholds; or
(iii) when effecting domestic or international wire transfers at or above the prescribed threshold.

(b) Continuous CDD Obligations under SDD

3.4 The application of SDD does not exempt an institution from CDD. Rather, it entails the implementation of reduced yet sufficient measures that adequately addresses all four core components of CDD that apply to "standard" customer relationships and transactions. In line with Section 19(1) and Section 20 of the FI Act, these CDD and anti-money laundering/ counter-finance terrorism/ counter-proliferation financing (AML/CFT/CPF) obligations include:

(i) Customer identification and verification - identifying the customer and verifying their identity using reliable, independent source documents, data, or information.
(ii) Beneficial ownership identification and verification - identifying the beneficial owner and taking reasonable measures to verify their identity, such that the institution is satisfied it knows who the beneficial owner is; for legal persons and arrangements, this includes taking reasonable measures to understand the customer's ownership and control structure.
(iii) Understanding the purpose and intended nature of the business relationship or transactions – obtaining sufficient information to understand the rationale, expected activity, and anticipated use of the account or service.
(iv) Ongoing monitoring of business relationship as pursuant to Section 19(1) of the FI Act – continuous conduct of CDD with respect to an existing business relationship which includes:

a. periodic review of accounts to maintain current information of records relating to the customer and beneficial owners, where reviews may be initiated on a periodic basis or in response to specific triggers, such as significant changes in a customer's transaction behaviour, new high-risk factors (e.g. the customer obtaining additional products or services, reaching pre-defined thresholds, or other indicators that may elevate risk), and;
b. scrutinising of transactions to confirm that the activity aligns with the institution's understanding of the customer, the intended purpose of the account, and the customer's overall risk profile.

3.5 Where a financial institution has determined that a customer is low risk, it may apply a reduced level of ongoing monitoring, both in frequency and intensity. In such cases:

(i) Customer identification information may be updated every five years, unless a trigger event requires earlier review; and

(ii) Transaction monitoring may be conducted less frequently and with a lower level of scrutiny, provided it remains sufficient to detect unusual or suspicious activity.

Similar CDD measures should be adopted for persons conducting transactions on behalf of a customer.

3.6 In instances where SDD measures are applied, the institution shall clearly document the rationale, including the underlying ML/TF/PF risk assessment that supports the determination. Moreover, all information, document or data obtained for the purpose of applying SDD should be recorded and maintained in line with the requirements of Section 31 of the FI Act.

3.7 Financial institutions are required to report any suspicious transactions that may arise from low risk rated customers on whom SDD measures are applied in accordance with Section 38 of the FI Act.

4. Application of Risk-based Approach (RBA)

4.1 Risk-based approach (RBA) is the process of identifying, assessing and understanding ML/TF/PF risks and taking commensurate due diligence measures in line with the customer risk profile in order to mitigate them effectively. Higher-risk situations should attract enhanced measures, while lower-risk situations may allow for simplified measures.

4.2 An institution should not automatically apply SDD measures to a "pre-defined" list of customers. Instead, consistent with the RBA an institution should actively demonstrate that the customer presents genuinely low risk and provide robust rationale for the application of SDD. In determining whether the application of SDD is appropriate, an institution should undertake risk assessments that consider, at minimum, the following factors:

(i) customer risk (e.g. resident or non-resident, type of customer, occasional or one-off, legal person structure, types of occupation, types of prominent influential person (PIP), etc.);
(ii) products, service, transaction or delivery channel risk (e.g. cash-based, face-to-face or non-face-to-face, cross-border, etc.);
(iii) country or geographical risk (e.g. location of business, origin of customer, etc.); or
(iv) other risk factors as may be determined by an institution (e.g. account type, financial inclusion objectives, institution's business strategy, and ownership structure, etc.), or through the National Risk Assessment or by the Bank.

4.3 When assessing the ML/TF/PF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, a financial institution should consider risk variables relating to those risk categories. These variables, either individually or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Appendix 1 provides ML/TF/PF risk indicators to be considered when conducting risks ratings in relation to customers, geographic areas, products, practices and services offered, or delivery channels.

4.4 Risk-rating implies assigning different categories to different levels of risk according to a risk scale and classifying the ML/TF/PF risks pertaining to different relationships or client engagements in terms of the assigned categories. As no two financial institutions are the same,

the level of risk and the risk ratings attributed to particular business relationships or other engagements with clients may vary between financial institutions.

4.5 A risk scale should be tailored according to the size of the institution and consideration may be given to criteria set out in international best practice. The complexity of the risk scale should reflect the size and complexity of the institution and the nature and the range of products and services it offers to its clients.

4.6 Financial institutions offering a relatively homogenous range of products and services, using a limited range of delivery channels, operating in one or a few geographic location(s) or engaging with a homogenous range of clients require relatively simplistic risk scales distinguishing only between two or three risk categories. However, institutions offering a more diverse range of products and services, using a wider range of delivery channels, operating in a larger number of geographic locations or engaging with a more diverse range of clients require more finely calibrated risk scales distinguishing between a larger number of risk categories.

4.7 The ML/TF/PF risk associated with a particular client engagement is not static. The factors underlying any given risk-rating will inevitably change over time. It is, therefore, essential that institutions re-evaluate the relevance of particular risk factors and the appropriateness of previous risk-ratings from time to time and determine the intervals at which this will be done. The frequency of the risk-rating review may be based on the customer risk-score, where institutions will reduce the frequency of review for low risk rated customers.

4.8 Financial institutions must document the risk-rating methodology and procedures which they apply as well as the conclusions reached through the processes in the institution's AML/CFT/CPF Risk Management Compliance Programme (RMCP). The RMCP should also reflect the Board-approved risk appetite statement and the defined risk tolerance levels for ML/TF/PF risks. This includes the criteria and the intervals for the re-evaluation of risk-ratings.

(a) Customer Risk Factors

4.9 Not all customers qualify for SDD. Generally, customers with inherent low risk, such as certain types of businesses or individuals in specific sectors, may be eligible for SDD. Examples of when an institution might adopt lesser or reduced CDD measures include:[1]

(i) Botswana Government entities;
(ii) financial institutions and designated non-financial business professions (DNFBPs), as they are subject to requirements to combat ML/TF/PF consistent with the FI Act, and have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the requirements of the FI Act;
(iii) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.

[1] Generally, certain categories of customers listed below are considered low risk. However, if a financial institution determines that a specific entity listed in the examples presents an elevated risk of ML/TF/PF, it must apply standard or enhanced due diligence measures accordingly.

(b) Product, Service, Transaction or Delivery Channel Risk Factors

4.10 Every product, service, transaction or delivery channel poses a different level of ML/TF/PF risk. Examples of when such reduced measures may be considered include:

(i) Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes may be assigned lower risk-scores. These are products and services launched to provide appropriately defined and limited services to certain types of customers to serve financially excluded and underserved groups. Examples include "small bank/merchant accounts" for unbanked or underserved individuals who lack full verification documents, where limits are imposed on turnover, balances, transaction size, usage frequency, and international transfers. Such accounts can facilitate essential needs, such as receiving remittances or supporting small-scale business activity, while keeping ML/TF/PF exposure low.

(ii) a financial institution may also adopt a "progressive" or "tiered" CDD approach, where strict transaction or balance limits correspond to reduced ML/TF/PF vulnerabilities. Products with tighter limits are more likely to qualify for lower-risk categorisation and may justify the application of SDD. Access to additional features, such as higher limits or broader delivery channels, should be permitted, but must trigger the application of standard or enhanced CDD measures (EDD).

(iii) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.

(c) Country or Geographical Risk Factors

4.11 The jurisdiction in which a customer resides, operates, or conducts transactions can materially influence overall risk. Examples of lower-risk country or geographical factors include:

(i) countries identified by credible sources, such as mutual evaluation or detailed assessment reports (e.g. NRA), as having effective AML/CFT systems may be risk-rated low; and
(ii) countries identified by credible sources as having a low level of corruption or other criminal activity.

5. Application of Simplified Due Diligence

5.1 In circumstances where the risk of ML/TF/PF has been assessed to be low and provided there has been an adequate analysis of the risk by the financial institution, financial institutions should apply SDD measures.

5.2 SDD does not mean a complete exemption or absence of CDD measures but requires a basic and minimal set of CDD measures, that must still respond to each of the four CDD components that apply to standard and EDD measures. In line with the RBA, it is the intensity and the extent of customer and transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level.

5.3 In the application of SDD, a financial institution could:

(a) reduce identification and verification requirements – accepting the following documents for identification of customers and beneficial owners
  (i) national identity card for Batswana,
  (ii) national identity card for foreigners from specified countries,
  (iv) passport for foreigners,
  (v) certified or notarized foreign national identity for a foreign customer who does not have a passport, and
  (vi) refugee identity card.

(b) verify the identity of the customer and the beneficial owner after the establishment of the business relationship

  (i) delayed verification[2] may be enabled, provided that only limited, low-value services are offered until full verification is completed. This deferred-verification approach enables access to basic accounts for unbanked or underserved individuals while maintaining appropriate safeguards. It reduces onboarding barriers and costs for small-value accounts, supports financial inclusion, and ensures that expanded services or higher transaction limits are granted only once full CDD is completed.

  (ii) reduce the frequency of customer identification updates and the degree of on-going monitoring and scrutinising transactions.

(c) financial institutions should monitor lower-risk accounts but may do so with reduced frequency and intensity than standard-risk or high-risk accounts, allowing resources to be prioritised toward higher-risk areas.

(d) understand the purpose and nature of the business relationship by inferring to the type of customer transaction or business relationship that has been established and be adjusted in line with the customer behaviour patterns;

(e) identify and/ or verify the beneficial owner using information obtained from the customer's profile.

6. Simplified Due Diligence for Different Types of Customer

6.1 In all situations of SDD, the lower risk circumstances will have to be confirmed based on a thorough and documented risk assessment, conducted by the financial institution. Financial institutions are required to specify the different criteria required to benefit from a SDD regime within their own risk management framework.

[2] Verification must be concluded within 30 days of client onboarding. During this period, financial institutions should apply strict transactional caps, restrict usage to domestic transactions, and automatically suspend the account if verification has not been completed within the prescribed timeframe

6.2 In any case, SDD is not permitted if there is any suspicion of money laundering, or terrorist financing, or where specific higher-risk scenarios apply.

(a) Natural Persons/ Individuals

6.3 Where a financial institution seeks to establish the identity of a natural person, and has through the risk assessment conducted determined that the customer is a low-risk, or the customer opening the account is a low-income customer, the financial institution shall establish and verify the identity of a customer through one of the following:

(i) national identity card for Batswana,
(ii) national identity card for foreigners from specified countries,
(vii) passport for foreigners,
(viii) certified or notarized foreign national identity card for a foreign customer who does not have a passport, and
(ix) refugee identity card.

6.4 When establishing the customer's identity under an SDD regime, the financial institution shall obtain and maintain, at a minimum, the following information:

(i) the person's full legal names;
(ii) the person's nationality;
(iii) the person's gender and title;
(v) where the person is a citizen or resident of Botswana,
(vi) place and date of birth of such person;
(vii) the person's residential address in Botswana and person's contact details;
(viii) where the person is not citizen or resident of Botswana,
(ix) the passport number (or foreign national identity number, if used); and
(x) place and date of birth of such person;
(xi) the residential address in his or her country of domicile and physical address in
(xii) Botswana and person's contact details;
(ix) where the person is a refugee, a refugee identity card number and date of birth of such person; and the person's contact details;
(x) the person's source of income;
(xi) For mobile money service providers obtain a registered cell phone number.

6.5 Any information or particulars ascertained by a financial institution should be verified against reliable, independent and unexpired official documents, namely:

(i) national identification issued by Botswana (Omang);
(ii) passport for foreigners that bears a photograph of the customer;
(iii) a refugee identity card; and
(iv) certified or notarized foreign national identity card for eligible foreign customers.

6.6 For SDD purposes, institutions should not request documentary proof of residential address or income. These details may be self-declared in the application form, consistent with the lower-risk profile and reduced verification requirements permitted under SDD.

(b) Legal Persons

6.7 In considering the customer identification guidance for the different types of legal persons, particular attention should be given to the different levels and nature of risk associated with these entities.

6.8 Regarding beneficial ownership requirements, in a financial inclusion context the beneficial owner will in most instances be the customer him/ herself. Situations where suspicions arise that the account holder is used as a strawman, or frontman and is not the real owner, should not be treated as low risk and standard or enhanced measures should be applied.

6.9 Where a financial institution seeks to establish the identity of a legal person under an SDD regime, and has, through its risk assessment, determined that the customer is low-risk or is opening a small bank/merchant account for low-income customers, the institution shall ascertain the following information:

(i) the registered name, legal form, and registration number of the body corporate;
(ii) the address from which it operates in Botswana, or outside Botswana;
(iii) the nature of business of the body corporate;
(v) identity of a natural persons as per the particulars referred to in Paragraph 6.4, whichever is applicable concerning:

a. the managers of the company,
b. natural persons who have authority to act on the account (that is signing authority),
c. natural persons who have authority to establish a business relationship or conclude a transaction with a financial institution on behalf of the company,
d. the natural person on whose behalf the transaction is concluded,
e. natural persons who either directly or indirectly hold more than 10 percent shares, voting right or other ownership interest; (in a majority of cases companies which are rated low risk do not have complex ownership structures), and
f. natural persons who have effective control over the company.

6.10 The financial institution should verify the identity of the customer established through information collected using reliable, independent source documents, data or information, namely:

(i) a copy of the certificate of incorporation and memorandum and articles of association, or partnership agreement (or any other legal document certifying the existence of the entity, e.g. abstract of the registry of companies from the Company and Intellectual Property Association Online Business Registration System (CIPA OBRS); or
(ii) a copy of the hawker's license issued by a local authority or city council, where the business is not registered with CIPA, or
(iii) where the business has not been registered with CIPA or any local authority (that is very small businesses) a self-declaration of the nature of the business and source of income will be sufficient.

(c) Non-Profit Organisations (Societies)

6.11 Where a financial institution seeks to establish the identity of a customer who is a Non-Profit Organisation (NPO) under an SDD regime, and has, through the risk assessment conducted, determined that the customer is a low risk, or the customer is opening a small bank/merchant account, the financial institution shall ascertain the following:

(i) registered name of the NPO;
(ii) physical operating address and contact details
(iii) nature and purpose of the NPO;
(vi) persons exercising control or significant influence over the organisation's assets should be identified and verified. This include board members and executives;
(vii) names of account signatories; and
(viii) source of funds.

6.12 A financial institution should verify the identity of the customer established through information collected using reliable, independent source documents, data or information, namely:

(i) a copy of registration certificate obtained from the relevant registry;
(ii) verification of identity of account signatories through identification documents prescribed under paragraph 6.3.

6.13 For SDD purposes, institutions should not request documentary proof of address, source of funds and verification of controllers where the NPO has been assessed to have a low risk of financial crime. These details may be self-declared in the application form, consistent with the lower-risk profile and reduced verification requirements permitted under SDD.

(d) Trust Entities

6.14 Where a financial institution seeks to establish the identity of a customer who is a trust entity, and has, through the risk assessment conducted, determined that the customer is low risk, the financial institution shall ascertain the following:

(i) full names of the trust, its registration number, its previous names and sub-trusts, if any;
(ii) date on which the trust was set up;
(iii) jurisdiction where the trust was set up and the manner of its creation, whether by trust instrument or otherwise;
(iv) place where the trust is administered;
(vi) a statement of account of the trust, describing the trust assets and identifying the value of each category of the trust assets;
(vii) source of funds used to acquire trust assets;
(viii) particulars referred to in Paragraph 6.4, whichever is applicable, in relation to each individual and entity in the trust, including the settlor, trustee, beneficiaries, protector, if any, and the natural person exercising ultimate effective control over the trust.

6.15 Any information or particulars ascertained by a financial institution in relation to a trust shall be verified using reliable, independent, and unexpired documents, namely:

(i) a trust instrument or deed of trust;
(ii) letters of authority issued to the trustees;
(iii) identification documents prescribed under paragraph 6.3 for trustees, settlors or protectors if any;
(iv) the financial institution needs not verify the identities of beneficiaries, except at the time of payout.

6.16 Beneficiaries of the trust need not be verified at onboarding and shall only be subject to identity verification at the time of payout.

7. Triggers Requiring Escalation from SDD to Standard or Enhanced Due Diligence

7.1 Financial institutions must conduct ongoing monitoring of all customers, including those assessed as low risk, to identify unusual or suspicious activity or any change in expected transactional behaviour. The emergence of such indicators necessitates a reassessment of the customer's risk profile and may require the application of standard or EDD measures.

7.2 The following circumstances constitute key triggers requiring financial institutions to transition from SDD to either standard or EDD measures:

(i) change in customer risk profile - where a customer initially assessed as low risk begins to exhibit behaviours or characteristics associated with higher risk (e.g. unusual transaction patterns, increased transaction volumes, or use of complex ownership structures, frequent changes in company ownership structure or frequent changes in settlement bank accounts), the institution should reassess and potentially apply standard or EDD measures;
(ii) involvement with high-risk jurisdictions - where any transaction or business relationship is identified to involve countries subject to FATF grey/ blacklistings or possess strategic AML/CFT deficiencies, the institution must automatically trigger EDD measures;
(iii) change in prominent influential person (PIP) status - where a customer becomes a PIP during the course of a business relationship, the institution should apply EDD measures, consistent with the requirements of Section 22 of the FI Act;
(iv) adverse media or sanctions hits - where the customer is involved with adverse media, criminal records, or inclusion on sanctions/watchlists during ongoing monitoring, the institution should apply EDD measures.
(v) non-face-to-face transactions without adequate controls – while FATF allows non-face-to-face onboarding under SDD, if digital identity tools are used, lack of robust verification mechanisms (e.g. digital identity systems that do not meet an appropriate assurance level for identity proofing, authentication, and liveness verification) may trigger standard or EDD measures.
(vi) unusual or complex transactions - where any transactions that are inconsistent with the customer's known profile (e.g. large and frequent cash movements, etc.), the institution should trigger EDD measures.
(vii) beneficial ownership concerns - where the beneficial owner cannot be clearly identified or verified, or if ownership structures are deliberately obscured, the institution should apply standard or EDD measures.

(viii) customer association to high-risk business - where the customer is operating in sectors deemed high-risk (e.g. virtual assets, offshore finance, or gaming, etc.), the institution should apply standard or EDD measures.

(ix) regulatory or supervisory alerts - where there are guidelines or directives from the Bank or the Financial Intelligence Agency indicating elevated risk relating to a specific customer segment, sector, geography, the institution should prompt reassessment and potential standard or EDD measures.

8. Prohibition for Conducting SDD

8.1 In accordance with Section 28(3) of the FI Act, a financial institution shall not apply SDD measures in any of the following circumstances, where:

(i) there is suspicion of a commission of a financial offence;
(ii) based on the institution's risk assessment, the business relationship or transaction no longer presents a low risk of a financial offence;
(iii) the institution has doubts regarding the veracity or accuracy of any identification or verification information previously obtained; or
(iv) the customer's transaction or balance thresholds exceed those prescribed for low-risk customers eligible for SDD.

8.2 Standard CDD or SDD shall also be prohibited in any of the circumstances set out in Section 21 of the FI Act, including where:

(a) there is a high risk of commission of a financial offence identified through the institution's or supervisory authority's risk assessment;
(b) the business relationship or transaction established involves a high-risk jurisdiction or is initiated at the request of an international organisation;
(c) the transaction relates to a high-risk business activity;
(d) the customer is a PIP;
(e) the transaction is complex or unusually large, involves an unusual pattern, or lacks an apparent economic or lawful purpose;
(f) the FATF has advised that countermeasures or enhanced measures be applied in respect of a jurisdiction posing a threat to the international financial system; or
(g) the customer is known to present high-risk characteristics, including residence in high-risk jurisdictions or involvement in legal arrangements with opaque or complex ownership structures.

9. Effective Date

9.1 The guideline shall come into effect on 1 March 2026.

Appendix 1: Application of RBA in Customer Profiling

A1.1 In accordance with Paragraph 4.2, financial institutions are expected to adopt RBA in assessing the risk profile of a customer, which will then support the determination of applicability of simplified, standard or enhanced CDD measures. Such customer risk profiling is predicated on a documented, risk-sensitive evaluation of factors set out in Paragraph 4.2:

(i) customer risk;
(ii) products, service, transaction or delivery channel risk;
(iii) country or geographical risk; or
(iv) other risk factors as may be determined by an institution.

A1.2 These risk factors are intended to help institutions identify characteristics that may increase or decrease the level of ML/TF/PF risk posed by a customer or business relationship. They serve as a reference point to guide institutions in applying proportionate CDD measures consistent with Paragraph 4 recognising that RBA requires the aggregation and interpretation of multiple risk indicators, individually and in combination, when determining overall risk.

A1.3 Institutions should consider these illustrative factors alongside their own internal risk assessments and the NRA. These factors must be applied dynamically throughout the business relationship and should inform both initial customer risk classification and ongoing monitoring, including any re-rating of customer risk profiles. Refer to the following tables below for illustration purposes of the respective ML/TF/PF risk factors[3].

[3] The listed factors are for illustrative purposes only. The list is not exhaustive and should be applied proportionately to support risk-based implementation.

(a) Customer Risk Factors

Risk Factor Categories	**Subcategories**
Type of Customer	Natural Person
	Legal Person
	Legal Arrangement (e.g. Societies, Trust Entities, etc.)
Ownership / Control Structure	Simple ownership (≤10% beneficial ownership layers)
	Multi-layered, opaque or complex structure
	Use of nominees / proxy shareholders
Source of Income	Salaried / clearly documented income
	Self-employed / micro-SME with limited documentation
	Cash-intensive or unverifiable sources
Nature of Business Activity	Low-risk regulated sectors
	Unregulated sectors with normal cash intensity
	High-risk or cash-intensive sectors, precious metals, cross-border trade, NGOs in conflict zones)
Product and Service Relationship	Product usage consistent with stated personal/ business needs
	Occasional inconsistencies in product selection
	Product usage inconsistent with profile (e.g. high-value transfers in low-income profile)
Geographical Footprint of Customer	Operates solely domestically
	Cross-border operations in neutral jurisdictions
	Cross-border operations in high-risk or sanctioned jurisdictions
Prominence / PIP Status	Non-PIP
	Domestic PIP

	Foreign PIP or PIP in high-risk jurisdiction
Adverse Information	No adverse media
	Adverse media unverified or historical
	Active adverse media, sanctions exposure
Regulatory Compliance Profile	Subject to effective AML/CFT supervision
	Minimal supervision / weak regime
	Previously penalised for AML/CFT failures
Relationship Length	Established long-term customer with stable profile
	New customer (≤6 months)
	New customer, with unusual early activity
Transactional Behaviour	Activity consistent with profile
	Occasional deviations
	Unusual patterns, complex or rapid movement of funds
History of Suspicious Transaction Reporting (STR)	No prior STRs or alerts
	Internal alerts resolved satisfactorily
	Previously filed STR or repeated alerts

(b) Product, Service, Transaction Risk Factors

Risk Factor Categories	**Subcategories**
Anonymity	Full KYC required or some part waivered (e.g. financial inclusion products)
	High anonymity potential (e.g. prepaid anonymous instruments)
Funding Method	Funded through banking channels only
	Cash deposits allowed within limits
	Heavy cash inflows or cash-only funding
Third-Party Use	Product restricted to account holder only
	Permits limited third-party payments
	Broad third-party payment capability
Cross-Border Capabilities	Domestic use only
	Limited cross-border
	Full cross-border transfers
Regulatory Oversight	Fully regulated, regime stable
	Regulated but with gaps or transitioning
	Unregulated or weakly regulated
Transaction Limits	Tight daily / monthly caps
	Moderate limits
	High or no limits

Product Complexity	Straightforward (e.g., basic savings/current/merchant)
	Moderate complexity (e.g. insurance, investment-linked)
	Complex or structured (e.g. derivatives, FX margin, commodities)
Target Market	Low-risk segments (salaried, retirees, minors)
	SMEs / self-employed
	High net worth individuals, high-risk businesses
Cash Conversion Potential	Low (limited withdrawal options)
	Moderate
	Easy and rapid cash-out
Transaction Volume	Low
	Moderate
	High / high-velocity transactions

A1.4 Financial products or services with clearly defined and limited functionalities, especially those designed for unbanked or underserved customers, may warrant lower ML/TF/PF risk scores where built-in restrictions minimise opportunities for misuse. Consistent with Paragraph 4.10(i), such products typically feature limits on transactions, usage frequency, access channels, and cross-border capability. The following table provides illustrative examples of these account types and their limitations, demonstrating how structured product design can support low-risk categorisation under an RBA:

Accounts	**Restricted Features**
Basic Bank Accounts (Low-value savings, current, transactional, merchant accounts often used for financial inclusion)	• No overdraft facility • Low transaction limits • No international transfers • Low limits on monthly aggregate of cash withdrawals and transfers • Low limits on balances
Mobile Money Wallets (Digital stored-value accounts enabling basic payments and transfers within set limits)	• Transaction caps (e.g. daily or monthly limits) • No cross-border functionality • Restricted cash-out options • No international transfers
Government-to-Person (G2P) Payments (Accounts used for government disbursements such as welfare, pensions, or subsidies)	• Social welfare grants • Pensions • Disability allowances
Closed-loop Payment Cards (Pre-funded payment instruments with low limits and restricted, domestic-only usage)	• Low load limits • No reload or cash withdrawal features • Domestic use only

(c) Delivery Channel Risk Factors

Risk Factor Categories	**Subcategories**
Onboarding Method	Face-to-face onboarding – Directly with the institution
	Face-to face onboarding done by a third-party (Agent)
	On-line onboarding though USSD and other digital platforms
	Non-face-to-face onboarding with strong digital ID & liveness verification
	Non-face-to-face onboarding without robust verification
Intermediary Involvement	No intermediary (direct institution–customer interaction)
	Intermediary involved but licensed/regulated
	Unregulated, opaque, or informal intermediaries used
Transaction Execution Channel	Transactions conducted directly with institution
	Transactions routed via regulated agents or authorised channels
	Transactions routed via unregulated third parties or distributed networks
Platform / Technology Environment	Secure, institution-controlled platform
	Mixed-use platforms (third-party interfaces with adequate oversight)
	High-risk platforms or exchanges with limited regulatory control
Market Type	Not traded on exchanges
	Traded on regulated exchanges
	Traded on secondary or informal markets

Payment System Integration	Simple payment rails owned/controlled by institution
	External payment rails with moderate oversight
	Use of unregulated or high-risk payment systems
Institutional System Dependency	Low reliance on institution systems (simple, low-volume)
	Moderate reliance (standard digital channels)
	High reliance (complex, automated, multi-party systems)

(d) Country or Geographical Risk Factors

Risk Factor Categories	**Subcategories**
Country of Domicile / Operation	Botswana or low-risk jurisdiction
	Neutral or moderately regulated jurisdictions
	High-risk / sanctioned jurisdictions
Engagement Footprint	Customer operates only domestically
	Customer operates regionally
	Customer operates across high-risk zones
Regulatory Strength	Strong AML/CFT framework
	Moderate AML/CFT framework
	Weak AML/CFT supervision
Beneficial Ownership Transparency	High transparency jurisdictions
	Moderate transparency
	Known secrecy havens
Sanctions Exposure	No sanctions
	Indirect exposure via counterparties
	Direct sanctions listing or high sanctions jurisdiction

A1.5 The illustrative risk factors provided in this Appendix are not exhaustive and are not prescribed as mandatory parameters. Financial institutions are expected to determine which risk factors are most relevant based on the nature, size, complexity, and risk exposure of their business, the characteristics of the clients they serve, and the products and services they offer.

A1.6 Institutions should design risk rating models that reflect their operational complexity, delivery channels, geographical footprint, and customer base. A simple three-tier risk classification (e.g. low, medium, high) may be adopted for low-risk financial institutions, while a more granular models (e.g. four-tier or five-tier risk scales) may be adopted for complex and sophisticated financial institutions.

A1.7 Institutions may adopt similar risk factors and parameters used in broader sectoral or institutional assessments, including those identified under the NRA, where relevant and appropriate.

A1.8 Identification of a single high-risk indicator does not automatically render a customer high risk. The RBA requires institutions to analyse risk factors collectively, taking into account the customer's transactional behaviour and the evolution of risk throughout the business relationship.

A1.9 Institutions must ensure that CDD information collected during onboarding and through ongoing monitoring is accurate, relevant, and up to date, and that risk ratings are reviewed at intervals appropriate to the assessed level of risk.

Issued this ……**24th** ……...… day of ……**February**…….……..…,2026

DIRECTOR
BUSINESS CONDUCT AND REGULATORY COMPLIANCE DEPARTMENT

Acronyms and Abbreviations

Abbreviation	Full Phrase
AML/CFT/CPF	Anti-Money Laundering/Counter Financing of Terrorism/Counter Proliferation Financing
CDD	Customer Due Diligence
CIPA	Company and Intellectual Property Association
DNFBPs	Designated Non-Financial Business Professions
FI Act	Financial Intelligence Act, 2022
FATF	Financial Action Task Force
ML/TF/PF	Money Laundering, Terrorism Financing and Proliferation Financing
NRA	National Risk Assessment
NPO	Non-Profit Organizations
PIP	Prominent Influential Person
RMCP	Risk Management Compliance Programme
RBA	Risk Based Approach
SDD	Simplified Due Diligence
STR	Suspicious Transaction Reporting