Bank of Papua New Guinea

Prudential Standard BPS253: Customer Due Diligence Standards

Issued under Section 27 of *the Banks and Financial Institutions Act* 2000

Overview and Key Requirements

Papua New Guinea is a member of the Asia Pacific Group on Money Laundering (APG), and has committed to implement programs to prevent PNG's financial system from being used for money laundering or terrorist financing activities.

The Financial Action Task Force's (FATFs) 40 Recommendations are international standards that PNG has chosen to implement by virtue of its membership with the Asia Pacific Group (APG) on Money Laundering. APG is an autonomous and collaborative international organization founded in 1997 and consists of members within the Asia-Pacific region and a number of international and regional observers. One of the key objectives of the APG is to participate in, and co-operate with, the international anti-money laundering network - primarily with the FATF and with other regional anti-money laundering groups by ensuring that its member countries are implementing and complying with the internationally FATF requirements.

This prudential standard is also designed from the backdrop of the Bank of International's (BIS)/Basel Committee's 2011 revised, *"Core Principles of Effective Banking Supervision."* In particular, C*ore Principle 29- Abuse of Financial Services.*

Beyond meeting obligations under international financial relationships, strong anti-money laundering measures support efforts to reduce corruption and tax avoidance and protect against PNG being used for criminal activities. The requirements under this Prudential Standard are consistent with the Proceeds of Crime Act 2005 (POCA) and regulations.

This Prudential Standard aims to ensure that each Authorised Institution (AI) documents and implements robust Know Your Customer (KYC) and anti-money laundering processes, meets obligations under the POCA and Financial Intelligence Unit (FIU) guidelines and operates to prevent the AI from being used to facilitate money laundering, corruption, tax avoidance and other criminal activity including terrorist financing. Greater understanding of customers and their financial arrangements through KYC procedures, also assists the Authorised Institution to develop and fine tune risk management processes.

The key requirement is that an Authorised Institution must implement a documented KYC and AML policies and procedures that incorporate:

- Customer Acceptance Policy,
- Customer Identification Procedures,
- Monitoring of Transactions, and
- Risk management.

In addition, each Authorised Institution must implement a program to review and remediate existing customer files to ensure appropriate risk categorization, completeness of files including identification of beneficial ownership, sources of wealth and political exposure.

Application

1. This Prudential Standard applies to each Bank and Licensed Financial Institution authorized under the Banks and Financial Institutions Act 2000 (**BFIA** which are collectively referred to as Authorised Institutions (**AIs**) for the purposes of this prudential standard.
2. It is a condition of the license of each AI and also responsible person to ensure that the AI complies with all requirements of this Prudential Standard.
3. This Prudential Standard should be read in conjunction with:
   a. The Proceeds of Crime Act (2005); and
   b. Guidelines issued by the Papua New Guinea Financial Intelligence Unit under Section 14 (c) of the Proceeds of Crime Act 2005

Definitions

4. Refer to BPS 001 Bank of Papua New Guinea Prudential Standards – Glossary and Definitions for a complete set of definitions and glossary of terms used in this Prudential Standard. Defined terms are hyperlinked in the electronic version of this Prudential Standard.
5. For the purposes of this prudential standard, a 'Customer' is:
   a. a person or entity that opens, closes, operates or maintains an account, conducts a transaction and/or has a business relationship with the AI;
   b. a person on whose behalf the account is maintained (i.e. the beneficial owner) even if that person's identity is unknown to the AI;
   c. beneficiaries of transactions conducted by professional intermediaries, such as chartered accountants, solicitors, stock brokers, trusts and similar;
   d. a person or entity connected with a wire transfer or electronic funds transfer as either sender, correspondent or beneficiary either domestically or internationally in which the AI is involved;
   e. a person or entity that engages in transactions involving high demand value demand drafts or cash or obtains a stored-value instrument from the AI;
   f. a person or entity that applies for, opens, holds or uses a deposit box;
   g. a person or entity that obtains or holds a loan or mortgage;
   h. a person or entity who transacts on a third party account or conducts transactions on behalf of another person or entity; and
   i. a person or entity who attempts to do any of the above but is rejected or refused by the AI.
6. For the purposes of KYC a "politically exposed person" is:
   a. a natural person who is or has been entrusted with prominent public functions whether in PNG or a foreign country;
   b. immediate family members of such a person; or

c. associates of such a person, where "prominent public functions" includes the roles held by a head of state or province, a head of government, government ministers, senior and/or influential civil servants/officials entrusted with control of significant government assets or important government administrative role, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

Principles and Prudential Requirements

Responsibility of Board and Senior Management

7. The Board of Directors (Board) is responsible for ensuring the AI meets its obligations under all relevant laws, regulations, prudential standards and reporting requirements associated with KYC and AML/CTF regulations in PNG and other jurisdictions in which the AI operates.

8. The Board must ensure that policies and procedures are comprehensive and implemented fully. This includes strict customer due diligence (CDD) rules to promote high ethical and professional standards in the AI to prevent it from being used.

9. Further, that all staff receive appropriate training including annual awareness training. The compliance and internal audit function must monitor and test the effectiveness of policies and procedures and their implementation.

10. The AI's KYC policies and procedures must address the following four elements:
    a. Customer Acceptance Policy (CAP),
    b. Customer Identification Procedures (CIP),
    c. Monitoring of transactions and accounts, and
    d. Compliance and risk management.

Customer Acceptance Policy (CAP)

11. The CAP must establish explicit criteria for acceptance of customers, and by definition the rejection of potential customers as well as separation with existing customers that do not meet the CAP. Policies and procedures are expected to provide:

    a. that no account is opened in an anonymous or fictitious name;

    b. accurate risk categorisation of customers as low, medium or high risks (or level I, II, or III etc) to provide for risk based monitoring of accounts and transaction and frequency of customer and enhanced due diligence processes. Parameters for risk categories must be clearly defined and at a minimum address nature of business activity, sources of wealth, location of customer and clients, mode of payments, volume of turnover, social and financial status etc as well as customers requiring very high level of monitoring, for example, Politically Exposed Persons (PEPs);

    c. that no account is opened and that existing accounts are closed where the AI cannot undertake appropriate customer due diligence measures. For example, the AI is unable to verify the identity and /or obtain documents required as per the risk categorisation due to uncooperative nature of the customer or unreliability of the data or information provided;

    d. criteria and verification requirements, where a customer is permitted to act on behalf of another person or entity, for example, trustee on behalf of beneficiaries; and

e. searches and checks of applicants pre-account opening so as to ensure the customer is not a known criminal and/or does not pose a significant money laundering risk due to links to criminals or credible information suggesting involvement in criminal behavior, or terrorist or otherwise associated with banned entities, activities or countries.

12. For the purpose of risk categorisation:

a. Low risk – individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and whose transactions conform to their KYC profile, may be categorised as low risk. For example, salaried employees, low value credit card accounts.

Customers categorised as low risk must be subject to due diligence not less than every 3 years, when their categorisation changes or if transactions or activities have triggered raising a suspicious transaction report.

b. Medium risk – categorisation as medium risk may be the aggregation of a number of characteristic around the customer's background, sources of wealth, nature and location of activity, country of origin, sources of funds, client profile, significant cash dealings, or substantial dealings with Government agencies or departments.

Customers categorised as medium subject to due diligence every 2 years, when their categorisation changes or if transactions or activities have triggered raising a suspicious transaction report.

c. High Risk – certain activities should be require high risk categorisation regardless of size, nature of transactions, verification etc and require enhanced due diligence on an annual basis, that is, every year. These include:

- Money changers, bullion dealers, money transfer agencies, payday lenders;
- Jewelry or gold dealers;
- Gaming establishments, nightclubs, bars;
- non-resident customers;
- high net worth individuals;
- trusts, charities, NGOs and organisations receiving donations;
- companies having close family shareholding or beneficial ownership;
- firms with 'sleeping partners';
- politically exposed persons (PEPs);
- law firms, real estate agents and other entities that operate trust accounts through which clients funds may be moved anonymously;
- non-face to face customers; and
- known criminals or those with dubious reputation as per public information available or individuals who are known to have been exited by other AI’s, etc.

d. BPNG acknowledges that it would be impossible to review all accounts under the risk categories within the required timeframes under each of those categories. It is intended that an AI must ensure that it has adequate programs, process and systems in place to adequately review and demonstrate that the risks posed by the different types of customers under the required timeframes of each risk class of high, medium or low are managed prudently and with the purpose of satisfactorily fulfilling its KYC obligations as required by this standard. The reviews must commensurate the AML/CFT risk appetite an AI inherits.

Customer Identification Procedures (CIP)

13. As part of KYC, the Board must establish clear CIP to be conducted at commencement of the client relationship, prior to certain financial transactions, as part of file remediation or customer due diligence (CDD) or enhanced due diligence (EDD).

14. At a minimum, the AI as part of its CIP must obtain evidence and record information of the customer, including but not limited to the following:

    a. full name, including any aliases;

    b. unique identification number and photographic identification (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number and a Taxpayer Identification Number (TIN));

    c. existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

    d. date of birth, incorporation or registration (as may be appropriate); and

    e. nationality or place of incorporation or registration (as may be appropriate).

    f. A TIN, for all High Risk customers, all individuals opening or operating an account under a business name, and all non-individual customers.

15. Where the customer is a company, the AI must also identify the directors of the company and the beneficial owners of the company. Where a beneficial owner is itself a company, the AI must identify the ultimate beneficial owner, that is, the natural person who owns or controls the company. Inability to properly identify or verify beneficial ownership should trigger actions under Section 20 (4) of the Proceeds of Crime Act 2005 and the AI must suspend the business relationship until such time as the beneficial ownership can be verified. Where the customer is a partnership or a limited liability partnership, the AI must identify the partners.

16. Where the customer is any other body corporate or unincorporated entity or trust or similar, the AI must identify all the persons having executive authority and also instruments for establishing that authority.

Verification of Identity

17. An AI must verify the identity of the customer using reliable, independent sources.

18. The AI must retain copies of all reference documents used to verify the identity of the customer.

19. Where the customer appoints one or more natural persons to act on his behalf in establishing business relations with the AI or the customer is not a natural person, the AI must:
    a. identify the natural persons that act or are appointed to act on behalf of the customer;
    b. verify the identity of these persons to act on behalf of the customer; and
    c. retain copies of all reference documents used to verify the identity and authority of these persons.

20. The AI must verify the due authority of such persons to act by obtaining at a minimum:
    a. appropriate reliable and independent documentary evidence, including an instruments of appointment or delegation, that the customer has appointed the person/s to act on its behalf.
    b. where the customer is a government agency, department or program or a state-owned enterprise, evidence must be obtained from a verifiable independent source such as instrument of appointment, Ministerial or Parliamentary confirmation, copy of gazette notice or similar; and
    c. the specimen signatures of the persons appointed.

Verification of Beneficial Owners

21. Where the customer is not a natural person, the AI must take reasonable measures to understand the ownership and control structure of the customer.

22. Where the customer is not a natural person, the AI must determine if there is a beneficial owner or controller of 20% or more of the customer.

23. Where there is one or more beneficial owners, the AI must obtain information sufficient to identify and verify the identities of the beneficial owners or ultimate beneficial owners.

24. The AI is not required to identify and verify any beneficial owner in relation to a customer that is:
    a. a Papua New Guinea government entity;
    b. a foreign government entity; and
    c. an entity listed on the POM Exchange and where its largest shareholdings do not exceed 10% of issued capital.

25. The AI must conduct CIP on managers and signatories of entities even if exempt under paragraph 24.

26. BPNG acknowledges that not all potential AI customers, particularly those in lower income groups, may have the required identification and documentation to meet CIP requirements. If a natural person belonging to low income group is not able to produce

documents to satisfy the AI about identity and address, the AI can open an account with that person on the following basis:

a. if the person has been introduced by another account holder who has been subjected to full KYC procedure; and

b. the person's relationship with the AI (all accounts) is not expected to exceed K1,000 and total transactions in a year are not expected to exceed K10,000; and

c. the introducer has maintained a relationship with the AI on good terms with no transaction concerns for a period of at least 1 year;

d. the customer provides a picture and address details certified by the introducer or any other evidence as to the identity and address of the customer to the satisfaction of the AI.

27. If at any point of time, the aggregate value of balances in all his/her accounts with the AI exceeds K1,000 or annual turnover exceeds K10,000, no further transactions will be permitted until the full KYC procedure is completed. The AI should notify the customer well ahead of reaching the thresholds to allow time to complete KYC administration.

28. In addition to conducting CDD measures, each AI must conduct EDD measures to identify and deal with customers who are, or are involved with a politically exposed person, including:

a. appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed PEP a PEP;

b. approval from the AI's senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP;

c. establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

d. conduct enhanced monitoring of transactions, accounts and other business relations with the customer; and.

e. exit the customer immediately at any time that the AI is unable to establish a legitimate source and/or application of the funds.

Account and Transaction Monitoring

29. Each AI must establish a systematic approach to monitor customers' account and transaction activity to ensure that the transactions are consistent with the AI's knowledge of the customer, its business and risk profile and, where appropriate, the source and application of funds.

30. Each AI must pay special attention to all complex or unusually large transactions or patterns of transactions that have no apparent or visible economic or lawful purpose.

31. Each AI must have a process for reasonably ensuring that customers who are convicted of financially motivated crime offences, or about whom there is credible information indicating their involvement in financially motivated crime, are identified and appropriate risk categorisation changes made and procedures applied, including exiting the customer where appropriate.

32. Where an AI uses automated monitoring software or outsources monitoring to a third party, the AI must ensure that parameters and thresholds are appropriate in the PNG context and known money laundering typologies. Further, that all material in relation to monitoring, thresholds and parameters as well as results of inquiries to customers regarding the background and purpose of a transaction is recorded and made available to the competent authorities.

33. Each AI must review periodically the adequacy of customer identification information held in respect of customers and beneficial owners and ensure information is up to date. Depending on the risk categorization, the frequency of reviews must be yearly (high risk), 2 yearly (medium risk) or 3 yearly (low risk). Reviews should also be triggered when there is a change to ownership, senior management, or a substantial change to expected transactions or activities or transactions that result in a suspicious transaction report.

34. Each AI must ensure that all branches and agents maintain proper records of all cash transactions of K10,000 and above – deposits and withdrawals and international funds transfers. The internal monitoring system must provide for the reporting of large cash transactions and any transaction of a suspicious nature.

35. Board endorsed policies and procedures must ensure proper implementation of KYC requirements including explicit responsibility for management oversight, systems and controls, segregation of duties, training, testing of compliance and other related matters.

36. The AI's internal audit and compliance functions must have clearly articulated responsibilities for evaluation of, and ensuring adherence to, the KYC policies and procedures.

37. The Board must ensure that the Internal Audit is staffed adequately and the scope and annual work plan of Internal Audit includes to check and to verify the application of KYC procedures at the branches and to comment on any lapses observed.

38. The AI must have initial and ongoing training of all staff in KYC processes and responsibilities with respect to anti-money laundering obligations. Training must be appropriate for staff responsibilities and activities. For example, frontline staff, compliance staff and staff dealing with new customers. All staff need to understand the reasons for KYC policies and procedures, the risks, how to implement policies consistently, detection and reporting of suspicious transactions and the risks and potential penalties. Training is expected to be updated regularly to reflect changing typologies.

Record Keeping

39. Each AI must prepare, maintain and retain documentation on all its business relations and transactions with its customers such that:

    a. all requirements imposed by the relevant laws and this Prudential Standard are met;

    b. any transaction undertaken can be reconstructed so as to provide, if necessary, evidence for prosecution of any criminal activity;

    c. BPNG or the FIU or other competent authority, the AI's compliance function and the internal and external auditors are able to review the transactions and assess the level of compliance with KYC and AML obligations;

    d. the AI can respond fully within a reasonable time or any more specific time period imposed by law, any enquiry or order from BPNG, the FIU or other competent authority regarding information related to an account or transaction; and

    e. documentation as originals or copies, in paper or electronic form or on microfilm, meet the tests for admissibility as evidence in PNG.

40. Each AI must implement record retention policies and procedures for periods not less than 7 years.

    a. following the termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

    b. following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

Notification Requirements

41. The AI, or its Auditors, must notify BPNG in writing of a material breakdown in KYC and AML procedures and implementation within 7 days of detection. Serious breaches are expected to be escalated within 24 hours. Implementation of an action plan to address weakness is not a substitute for urgent notification to BPNG.

Reporting

42. As part of its annual attestation to BPNG, the Board of the AI must provide assurances regarding continued compliance with all laws, regulations, prudential standards, code, rules and similar for each jurisdiction in which it operates.

Remedial Measures, Sanctions and Penalties

43. Non-compliance with this Prudential Standard or failure to implement appropriate KYC and AML systems and controls or willful or negligent disregard of the requirements of this Prudential Standard is an offence under section 54 of the BFIA. Penalties of up to K500,000 may apply if the AI fails to implement adequate KYC and AML measures as

required under this Prudential Standard. Continuing offences may be subject to further penalties of up to K5,000 per day. Such penalties are in addition to potential criminal charges and imprisonment.

44. If BPNG is not satisfied with the adequacy of an AI's systems and procedures for compliance risk management across the institutions, BPNG may vary the conditions of the AI's licence under section 14 of the BFIA. Such conditions may include, but are not limited, to:

    a. require immediate remediation of problem issues;

    b. suspend or limit certain business activities relating to identified weaknesses;

    c. prohibit certain transaction or a class of transactions; or

    d. require appointment of additional staff or third party support to address weaknesses identified.

Commencement

45. This prudential standard is effective immediately.

Appendix 1: At a minimum the acceptable evidence for the purposes of customer identification and verification

CIP requirement	Acceptable evidence
Individuals	
Legal name and any other names used or aliases	Passport • Unique Identification Card • Driving licence • Birth certificate • Photographic evidence for students • A Tax Identification Number (TIN) is mandatory for all "high risk" individuals and individuals opening or operating accounts under a business name, or conducting business transactions through individual accounts. Evidence of which must be a current Income Tax assessment notice upon which a TIN is quoted or a letter of confirmation of registration from the Internal Revenue Commission quoting the TIN
Correct permanent address	• Telephone bill • AI account statement • Utility Bill • Letter from employer (subject to satisfaction of the AI) Note: The AI's policies should require at least 2 forms of evidence if photo id included or 3 forms otherwise. Must be recent and original documents – no photocopies)
Companies	
Name of the company Principal place of business Street address of the company (no PO Box) Telephone / Fax Number	• Certificate of incorporation and Memorandum & Articles of Association • Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account • Power of Attorney granted to its managers, officers or employees to transact business on its behalf • Recent bank account statement • A TIN is mandatory for all companies. Evidence of which must be a current Income Tax assessment notice upon which a TIN is quoted or a letter of confirmation of registration from the Internal Revenue Commission quoting the TIN • Copy of licenses held • Copy of utility bill
Partnership Firms	

Legal name Street Address (No PO Box) Names of all partners and their addresses Telephone numbers of the firm and partners	• Registration certificate, if registered • Partnership deed • Identification for the partners • Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf • Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses • Utility bill in the name of firm / partners • A TIN is mandatory for all partnerships. Evidence of which must be a current Income Tax assessment notice upon which a TIN is quoted or a letter of confirmation of registration from the Internal Revenue Commission quoting the TIN.

Trusts & Foundations

Names of trustees, beneficiaries and signatories Names and addresses of the founder, the managers / directors and the beneficiaries Telephone / fax numbers	• Trust Deed and Certificate of registration, if registered • Power of Attorney granted to transact business on its behalf • Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders / managers / directors and their addresses • Bank account statements • Resolution of the managing body of the foundation / association • Utilities Bill • A TIN will be mandatory for all trusts and foundations. Evidence of which must be a current Income Tax assessment notice upon which a TIN is quoted or a letter of confirmation of registration from the Internal Revenue Commission quoting the TIN.