RESERVE BANK OF VANUATU

INTERNATIONAL BANKS

PRUDENTIAL GUIDELINE NO. 9

CUSTOMER DUE DILIGENCE

AUTHORIZATION

1. The Reserve Bank of Vanuatu (the Reserve Bank) is authorized to formulate guidelines and issue directives in relation to prudential matters to be complied with by licensees under Sections 13 (3) of the International Banking Act Cap 280 (the IBA).

2. This Prudential Guideline (PG) is applicable to all international banks licensed by the Reserve Bank under the IBA to carry on international banking business.

INTRODUCTION

3. Consistent with ensuring that banks operating in Vanuatu implement sound risk management practices, this PG sets out the Reserve Bank of Vanuatu requirements for all banks operating in Vanuatu with international banking business license to incorporate the principals and recommendations outlined in this Guideline into their risk management policies. The objective of this guideline is to ensure that international banks have in place know-your-customer (KYC) policies. This guideline is based on principles outlined by the Basel Committee on Banking Supervision in its paper, "*Customer due diligence for banks*" issued in October 2001.

4. In addition to the requirements of this guideline, banks are also expected to comply with the requirements of the IBA and the Anti-Money Laundering and Counter-Terrorism Financing Act No.13 of 2014 (AML/CTFA) and the Anti-Money Laundering and Counter Terrorism Financing Act Regulation Order No.122 of 2014

(AMLCTFRO). Section 2 of the AML/CTFA specifically defines the Reporting Entities that are subject to the AMLCTFA and AMLCTFRO, and section 9 of the AMLCTFA requires for the registration of each Reporting Entities with the Financial Intelligence Unit (FIU)

BACKGROUND

5. Internationally supervisors are increasingly recognizing the importance of ensuring that banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, international banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

6. KYC is most closely associated with the fight against money-laundering and terrorist financing. The Reserve Bank's approach to KYC is from a wider prudential, not just anti-money laundering or counter terrorist financing perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious transactions.

ESSENTIAL ELEMENTS OF KYC STANDARDS

7. All international banks are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the international bank from being used, intentionally or unintentionally, by criminal elements. Certain key elements should be included by international banks in the design of KYC programmes. Such essential elements should start from the international banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. International banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of the international banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

Customer acceptance policy

8. International banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to an international bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

International banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers.

Customer identification

9. Customer identification is an essential element of KYC standards. For the purposes of this guideline, a customer includes:

   - The person or entity that maintains an account with the international bank or those on whose behalf an account is maintained (i.e. beneficial owners);
   - The beneficiaries of transactions conducted by professional intermediaries; and
   - Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the international bank.

   This definition should be read in conjunction with the interpretation of "customer" in Part 1 of the AMLCTFA.

10. International banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

11. International banks should document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised and in no case should an international bank short-circuit identity procedures just because the new customer is unable to present for interview.

12. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, international banks should undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if an international bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

13. International banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the international bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking

relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, international banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers, supervisors and auditors.

14. International banks should develop clear standards on what records must be kept on customer identification and individual transactions and their retention period. Such a practice is essential to permit an international bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. International banks should obtain customer identification papers and retain copies of them for at least six years after the account is closed. As required under Section 19 of the AMLCTFA, international banks must keep records of every transaction that is conducted through it and must retain records for a period of six years after the completion of the transaction. Section 19 of the AMLCTFA also specifies the type of transaction data that must be retained by international banks. In line with the requirements outlined in section 19 of the AMLCTFA , an international bank must maintain records of:

    a) Its transactions and related documents[1];
    b) A person's identity
    c) All reports made to the Director of FIU;
    d) All enquiries relating to the money laundering and the financing of terrorism made to it by the FIU or a law enforcement agency

    The records must be kept for a minimum period of 6 years from the date

    a) The evidence of a person's identity was obtained;
    b) Of any transaction or correspondence;
    c) The business relationship ceases

15. International banks should subject transactions with customers in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or financing of terrorism to additional scrutiny to examine the background and purpose of the transaction.

GENERAL IDENTIFICATION REQUIREMENTS

16. International banks should obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

i.

[1] In addition to customer identification/verification information, records relating to transactions will generally comprise, contract price (s) and valuation (in the case of unit-linked insurance policies); destination of funds; date of transaction; and the form in which funds are offered and paid out

17. When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the international bank should close the account and return the monies to the source from which they were received. It may also be appropriate, if the international bank has reasonable grounds to suspect that the account may have been for illegal purposes, for the international bank to prepare a Suspicious Transaction Report (STR) and/or Suspicious Activity Report (SAR) and submit this report to the Director of FIU.

18. Section 37 of the AMLCTFA requires that international banks should include originator information and related messages on funds transfers that should remain with the transfer throughout the payment chain. Originator information should include name, address, and account number (when being transferred from an account). International banks should give enhanced scrutiny to inward funds transfers that do not contain originator information. Should problems of verification arise that cannot be resolved or if satisfactory evidence is not produced to or obtained by an international bank under section 12 of the AMLCTFA , the international bank should not proceed any further with the transactions unless directed in writing to do so by the Director of FIU and must report the attempted transction to the Director of FIU as a suspicious transaction.

19. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, international banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if an international bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

20. In terms of section 14 and 15 of the AMLCTFA, international banks must not open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from an international bank's compliance function or from supervisory authorities.

SPECIFIC IDENTIFICATION ISSUES

21. Section 16 of the AMLCTFA requires that international banks must identify a customer on the basis of official or other identifying documents and verify the identity of a customer on the basis of reliable and independent source documents, data or information, or other such evidence as is reasonably capable of verifying the identity of the customer. There are a number of more detailed issues relating to

customer identification, which are outlined below and also outlined in Clause 3 of the AMLCTFRO[2].

Personal customers

22. For personal customers, international banks need to obtain the following information:

- Name and/or names used,
- Permanent residential address,
- Date and place of birth,
- Name of employer or nature of self-employment/business,
- Specimen signature, and
- Source of funds.

23. Additional information would relate to nationality or country of origin, public or high profile position, etc. International banks should verify the information against original documents of identity issued by an official authority[3] (examples including identity cards, passports and photo driver's licence). Such documents should be those that are most difficult to obtain illicitly. Where there is face-to-face contact, the appearance should be verified against an official document bearing a photograph. Any subsequent changes to the above information should also be recorded and verified.

Corporate and other business customers[4]

24. For corporate and other business customers, international banks should obtain evidence of their legal status, such as an incorporation document, partnership agreement, association documents or a business licence. For large corporate accounts, a financial statement of the business or a description of the customer's principal line of business should also be obtained. In addition, if significant changes to the company structure or ownership occur subsequently, further checks should be made. In all cases, international banks need to verify that the corporation or business entity exists and engages in its stated business. The original documents or certified copies of certificates should be produced for verification.

Trust, nominee and fiduciary accounts[5]

25. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood.

i.

[2] Refer to Table A of Schedule 2.
[3] Refer to Clause 4 and Table B of Schedule 2 of the AMLCTFRO.
[4] Refer to Clause 3 (and Table A of Schedule 2) and Clause 4 (and Table B of Schedule 2) of the AMLCTFRO
[5] ibid

International banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries.

Corporate vehicles[6]

26. International banks should be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international companies, may make proper identification of customers or beneficial owners difficult. An international bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

27. International banks should exercise care in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies should be obtained. In the case of entities that have a significant proportion of capital in the form of bearer shares, extra vigilance is required. An international bank may be completely unaware that the bearer shares have changed hands. Therefore, international banks should put in place satisfactory procedures to monitor identity of material beneficial owners. This may require the international bank to immobilise the shares, e.g. by holding the bearer shares in custody.

Introduced business[7]

28. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some instances, international banks may rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, international banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. International banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or thatare unwilling to share copies of due diligence documentation.

29. As required under section 18 of the AMLCTFA international banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in

i. _____

[6] ibid

[7] ibid

this guideline. The ultimate responsibility for knowing customers always lies with the international bank. International banks should use the following criteria to determine whether an introducer can be relied upon:

- It must comply with the minimum customer due diligence practices identified in this guideline;
- The customer due diligence procedures of the introducer should be as rigorous as those which the international bank would have conducted itself for the customer;
- The international bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- The international bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the international bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the FIU, where appropriate legal authority has been obtained. In addition, international banks should conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

Client accounts opened by professional intermediaries[8]

30. When an international bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

31. International banks may hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. International banks may also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the international bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

32. Where the funds are co-mingled, the international bank should look through to the beneficial owners. There can be circumstances where the international bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base

i.
[8] ibid

as the international bank. International banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the international bank should apply the criteria set out in paragraph 29 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

33. Where the intermediary is not empowered to furnish the required information on beneficiaries to the international bank, for example, lawyers bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this guideline or to the requirements of the AMLCTFA or anti-money laundering legislation in other jurisdictions, then the international bank should not permit the intermediary to open an account.

Politically exposed persons

34. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

35. Accepting and managing funds from corrupt PEPs will severely damage the international bank's own reputation and can undermine public confidence in the ethical standards of Vanuatu's financial system. In addition, an international bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, an international bank can be exposed to charges of money laundering, if it knows or should have known that the funds stemmed from corruption or other serious crimes. In this regard, section 13 of the AMLCTFA imposes requirements on banks to satisfy themselves as to the bona fides of the transaction.

36. International banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. International banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

37. Under Clause 5(2)(a) of the AMLCTFRO, international banks must put in place appropriate risk-based systems and controls to adequately indentify and verify its customers including PEPs.

38. Under clause 5(3) of the AMLCTFRO must have in place risk-based systems and controls to deal with politically exposed persons who are customer and must include the enhanced customer identification process, enhanced customer verification and enhanced on-going diligence processes.

39. Under clause 5(4) the reporting entity must have in place appropriate risk based systems and controls to identify, verify and understand whether the customer or the beneficial owner of the customer is a politically exposed person or an immediate family member of a political exposed person or a close associate of a political exposed person.

Non-face-to-face customers[9]

40. International banks are on occasion asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. International banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

41. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, the Reserve Bank of Vanuatu expects that international banks proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

42. In accepting business from non-face-to-face customers:

- International banks should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview; and

- There must be specific and adequate measures to mitigate the higher risk.

Examples of measures to mitigate risk include:

- Certification of documents presented;

- Requisition of additional documents to complement those which are required for face-to-face customers;

- Independent contact with the customer by the international bank;

i. [9] ibid

- Third party introduction, e.g. by an introducer subject to the criteria established in paragraph 27; or
- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Correspondent banking

43. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if international banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

44. Section 36 of the AMLCTFA requires that international banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. International banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

45. In particular, international banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Furthermore, international banks should not open correspondent account with banks that deal with shell banks. International banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against money laundering and terrorist financing. International banks should establish that their respondent banks have due diligence standards consistent with the principles outlined in this guideline, and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

46. International banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 27.

ON-GOING MONITORING OF ACCOUNTS AND TRANSACTIONS

47. On-going monitoring is an essential aspect of effective KYC procedures. International banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, international banks are likely to fail in their duty to report suspicious transactions where they are required to do so under the AMLCTFA. The extent of the monitoring needs to be risk-sensitive. For all accounts, international banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert international banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

48. There should be intensified monitoring for higher risk accounts. Every international bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

- International banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. For example, the types of reports could include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the international bank.

- Senior management in charge of private banking business should know the personal circumstances of the international bank's high-risk customers and be alert to sources of third party information. A senior manager should approve significant transactions by these customers.

- International banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

REPORTING OF SUSPICIOUS TRANSACTION OR ACTIVITIES

49. Where an international bank suspects, has reasonable grounds to suspect or has information that a transaction or attempted transaction may be related to a money laundering offence or financing of terrorism, the financial institution must as soon as practicable after forming the suspicion but no later than 2 working days, report the transaction to the Director of FIU. This reporting requirement is outlined in Section 20 of the AMLCTFA.

50. Where an international bank suspects, has reasonable grounds to suspect or has information that an activity or attempted activity involves proceeds of crime or is related to terrorist financing, the international bank must as soon as practicable after forming the suspicion but no later than 2 working days, report the activity to the Director of FIU. This reporting requirement is outlined in Section 21 of the AMLCTFA.

51. If a prescribed entity under Clause 11 of the AMLCTFRO conducts or seek to conduct a transaction through or by using an international bank and such transaction or attempted transaction is deemed to be a suspicious transaction involving proceeds of crime or is related to terrorist financing, the international bank must make a report of the same to Director of FIU not later than 2 working days. This reporting requirement is outlined in Section 22 of the AMLCTFA.

52. Where an international bank has information in its possession concerning any transaction or attempted transaction which its suspects involves terrorist property, property linked to terrorists or terrorist organizations, the international bank must not later than 2 working days provide the report to Director of FIU. This reporting requirement is outlined in Section 23 of the AMLCTFA.

53. Where an international bank suspects that a transaction or attempted transaction is unusual, the international bank must report the same to Director of FIU not later than 2 working days. This reporting requirement is outlined in Section 24 of the AMLCTFA.

54. Where Suspicious Transaction Reports (STR) and/or Suspicious Activity Reports (SAR) are submitted to Director FIU, the concerned international bank must not proceed further with the transaction unless directed to do so by the Director of FIU.

55. Section 34 (1) of the AMLCTFA requires international banks to each appoint an AML and CTF compliance officer(s) to be responsible for ensuring the international bank's compliance with the requirements of the AMLCTFA and the AMLCTFRO. The AML and CTF Compliance Officer(s) may be responsible for reporting suspicious transactions to the Director of FIU.

56. Section 26 of the AMLCTFA states that a suspicious transaction report under section 20, 21, 22, 23 or 24 must:

(a) be in writing and may be given by way of mail, fax or electronic mail or such other manner as may be prescribed;
(b) be in such form and contain such details as may be prescribed;
(c) contain a statement of the grounds on which the international bank holds the suspicion; and
(d) be signed or otherwise authenticated by the international bank.

57. A suspicious transaction or activity report may be given orally, including by telephone, but a written report must be prepared in accordance with section 26 (3) of the AMLCTFA within 24 hours after the oral report is given. Refer to forms on Schedule 3 and 4 of the AMLCTFRO.

58. AML and CTF Compliance Officers should keep a register of all reports made to the Director of FlU and all reports made internally to them by employees.

59. Directors, officers and employees of international banks are prohibited from disclosing the fact that an STR or SAR or related information is being reported to the Director of FlU. If an international banks form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the customer due diligence (CDD) process. If the international bank reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may not choose to pursue that process, and should file an STR/SAR. International banks should ensure that their employees are aware of any sensitive to these issues when conducting CDD.

60. If satisfactory evidence is not produced to or obtained by an international bank under section 12 of the AMLCTFA, the international bank should not proceed any further with the transaction unless directed in writing to do so by the Director of FlU and must report the attempted transaction to the Director of FlU as a suspicious transaction.

61. International banks and their employees are protected under Section 43 of the AMLCTFA when complying with their obligations under the Act.

RISK MANAGEMENT

62. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the international bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the international bank for ensuring that the bank's policies and procedures are managed effectively. The channels for reporting suspicious transactions to the FIU as required under the AMLCTFA should be clearly specified in writing, and communicated to all personnel. International banks should establish internal procedures for assessing whether the international bank’s statutory obligations under the AMLCTFA require

the transaction and/or activity to be reported to the Director of FIU. Clause 5 of the AMLCTFRO outlines the appropriate risk-based system and controls.

63. In accordance with paragraph 52, the AML and CTF Compliance Officer is responsible for ensuring compliance with the AMLCTFA and AMLCTFRO.

64. International banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. The Reserve Bank of Vanuatu expects that an international bank's compliance function should provide an independent evaluation of the international bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management, the Board of Directors or, in the case of foreign bank branches appropriate officers outside Vanuatu, if it believes management is failing to address KYC procedures in a responsible manner.

65. Internal audit plays an important role in independently evaluating the risk management and controls, through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training.

66. Section 33 (2) of the AMLCTFA requires that banks have in place an AML and CTF Procedure Manual covering ongoing employee-training programme so that international bank employees are adequately trained in KYC procedures. International banks should put in place measures to ensure that employees are aware of domestic laws and regulations relating to money laundering and the financing of terrorism. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments.

67. External auditors also have an important role to play in monitoring international banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice. In terms of the IBA and International Banking PG 5 – Audit Arrangements, international banks' external auditors have obligations to report to the Reserve Bank that all prudential standards have been observed, including the requirements of this Guideline.

THE ROLE OF RESERVE BANK OF VANUATU

68. The Reserve Bank of Vanuatu has a responsibility to monitor that international banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Under its powers to conduct on-site examinations, provided for under Section 14 of the IBA[10], the Reserve Bank of Vanuatu will be

i.

[10] Section 14 of the International Banking Act No. 4 of 2002 provides for the Reserve Bank to carry out the followings:

a) inspect the premise and the business, within or outside Vanuatu, including the systems and controls, of relevant person;

seeking to satisfy itself that appropriate internal controls are in place and that international banks are in compliance with supervisory and regulatory guidance. The review process will include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts

IMPLEMENTATION OF KYC STANDARDS IN A CROSS-BORDER CONTEXT

69. The Reserve Bank of Vanuatu expects banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors.

70. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, internal auditors and compliance officers from both local and head offices as appropriate should support him.

iii. ---

b) inspect the assets, including cash, belonging to or in the possession or control of a relevant persons;

(a) examine and make copies of the records belonging to or in the possession or control of a relevant person, being records that are in the opinion of the Reserve Bank relate to the carrying out of international banking business by the relevant person.