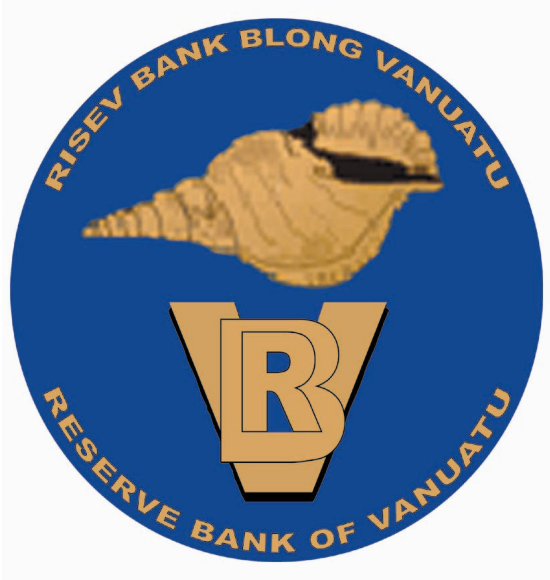

RESERVE BANK OF VANUATU

FINANCIAL INSTITUTIONS

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 21(2A) of the Financial Institutions Act CAP 254 (FIA).

2. This Prudential Guideline (PG) is applicable to all financial institutions licensed by the Reserve Bank to carry on banking business in Vanuatu and includes both domestic and foreign licensees as defined in the FIA. The Reserve Bank may also impose this PG to other financial institutions not licensed by the Reserve Bank, but are subject to Reserve Bank's supervisory and regulatory purview as stipulated under the FIA and/or their respective Acts.

INTRODUCTION

3. Consistent with ensuring that financial institutions operating in Vanuatu implement sound risk management practices, this PG sets out the Reserve Bank of Vanuatu's requirements for all domestic financial institutions and branches of foreign financial institutions to incorporate the principals and recommendations outlined in this Guideline into their risk management policies. The objective of this guideline is to ensure that financial institutions 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, financial institutions are also expected to comply with the requirements of the FIA, the Anti-Money Laundering and Counter-Terrorism Financing Act No.13 of 2014 (AMLCTFA), and the Anti-Money Laundering Counter Terrorism Financing Regulation Oder No. 122 of 2014 (AMLCTFRO). Section 2 of the AMLCTFA 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 financial institutions 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, financial institutions 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 financial institutions 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 financial institutions are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the financial institution from being used, intentionally or unintentionally, by criminal elements. Certain key elements should be included by financial institutions in the design of KYC programmes. Such essential elements should start from the financial institutions' risk management and

control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) ongoing monitoring of high risk accounts and (4) risk management. Financial institutions 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 financial institutions' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

Customer acceptance policy

8. Financial institutions 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 a financial institution. 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. Financial institutions 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 financial institution 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 financial institution.

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

10. Financial institutions should establish a systematic procedure for identifying new customers and should not establish banking or business relationship until the identity of a new customer is satisfactorily verified.

11. Financial institutions 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 in the case of non-resident customers and in no case should a financial institution short-circuit identity procedures just because the new customer is unable to present for interview. A financial institution should always ask itself why the customer has chosen to open an account in Vanuatu.

12. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, financial institutions 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 a financial institution 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. Financial institutions 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 financial institution 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, financial institutions 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. Financial institutions 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 a financial institution 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. Financial institutions 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 AMCTFA, financial institutions 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 and Clause 9 of the AMLCTFRO also specifies the type of transaction data that must be retained by financial institutions. In line with the requirements outlined in section 19 of the AMLCTFA , a financial institution 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

[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.

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. Financial institutions 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. Financial institutions 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.

17. When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the financial institution should close the account and return the monies to the source from which they were received. It may also be appropriate, if the financial institution has reasonable grounds to suspect that the account may have been for illegal purposes, for the financial institution 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 financial institutions 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). Financial institutions 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 a financial institution under section 12 of the AMLCTFA, the financial institution should not proceed any further with the transaction unless directed in writing to do so by the FlU and must report the attempted transaction to the Director of FlU as a suspicious transaction.

19. While the transfer of an opening balance from an account in the customer's name in another financial institution subject to the same KYC standard may provide some comfort, financial institutions 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 financial institution to another. However, if a financial institution has

any reason to believe that an applicant is being refused banking facilities by another financial institution, it should apply enhanced diligence procedures to the customer.

20. In terms of section 14 and 15 of the AMLCTFA, financial institutions 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 a financial institution's compliance function or from supervisory authorities.

SPECIFIC IDENTIFICATION ISSUES

21. Section 16 of the AMLCTFA and clause 4 of the AMLCTFRO[2] requires that a financial institution 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[3].

Personal customers

22. For personal customers, financial institutions 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. Financial institutions should verify the information against original documents of identity issued by an official authority[4] (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.

[2] Refer to Table B of Schedule 2

[3] Refer to Table A of Schedule 2

[4] Refer to Clause 4 and Table B of Schedule 2 of the AMLCTFRO

24. The Reserve Bank is aware that some personal customers (e.g. customers in rural areas or in the outer islands of Vanuatu) may not have some forms of identification documents referred to in paragraph 23 above. In such cases financial institutions may rely on other documents[5] (e.g. letters from Chiefs, Pastors, Magistrates, or Provincial Authorities) or other forms of independent identification. In doing so the onus remains on the financial institution to satisfy itself as to the customer's identity and to ensure that it fully understands the nature of such customers' transactions with the financial institution.

Corporate and other business customers[6],

25. For corporate and other business customers, financial institutions 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, financial institutions 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[7]

26. 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. Financial institutions 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[8]

27. Financial institutions 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. A financial institution 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.

---

[5] ibid

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

[7] ibid

[8] ibid

28. Financial institutions 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. A financial institution may be completely unaware that the bearer shares have changed hands. Therefore, financial institutions should put in place satisfactory procedures to monitor identity of material beneficial owners. This may require the financial institution to immobilise the shares, e.g. by holding the bearer shares in custody.

Introduced business[9]

29. 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, financial institutions may rely on the procedures undertaken by other financial institutions or introducers when business is being referred. In doing so, financial institutions 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 financial institution to know its customers and their business. Financial institutions should not rely on introducers that are subject to weaker standards than those governing the financial institutions' own KYC procedures or that are unwilling to share copies of due diligence documentation.

30. As required under section 18 of the AMLCTFA, financial institutions 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 this guideline. The ultimate responsibility for knowing customers always lies with the financial institution. Financial institutions 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 financial institution would have conducted itself for the customer;
    - The financial institution must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
    - The financial institution 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 financial

[9] ibid

institution, 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, financial institutions 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[10]

31. When a financial institution 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.

32. Financial institutions often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Financial institutions 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 financial institution, 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.

33. Where the funds are co-mingled, the financial institution should look through to the beneficial owners. There can be circumstances where the financial institution 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 as the financial institution. Financial institutions 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 financial institution should apply the criteria set out in paragraph 30 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

34. Where the intermediary is not empowered to furnish the required information on beneficiaries to the financial institution, 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 and counter-terrorism financing legislation in other jurisdictions, then the financial institution should not permit the intermediary to open an account.

[10] ibid

Politically exposed persons

35. 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.

36. Accepting and managing funds from corrupt PEPs will severely damage the financial institution's own reputation and can undermine public confidence in the ethical standards of Vanuatu's financial system. In addition, a financial institution 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, a financial institution and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes. In this regard, Section 53 of the FIA and Section 13 of the AMLCTFA imposes requirements on financial institutions and their officers to satisfy themselves as to the bona fides of the transaction.

37. Financial institutions 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. Financial institutions 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.

38. Under clause 5(2)(a) of the AMLCTFRO, financial institutions must put in place appropriate risk-based systems and controls to adequately indentify and verify its customers including PEPs.

39. 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.

40. 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[11]

41. Financial institutions 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. Financial institutions should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

42. 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 financial institutions proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

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

- Financial institutions 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 financial institution ;
- Third party introduction, e.g. by an introducer subject to the criteria established in paragraph 30; or
- Seeking verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds.

Correspondent banking

44. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent financial institutions have no physical presence. However, if financial institutions 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

[11] ibid

themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

45. Section 36 of the AMLCTFA requires that financial institutions should gather sufficient information about their respondent financial institutions to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent financial institution'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 financial institution regulation and supervision in the respondent's country. Financial institutions should only establish correspondent relationships with foreign financial institutions that are effectively supervised by the relevant authorities. For their part, respondent financial institutions should have effective customer acceptance and KYC policies.

46. In particular, financial institutions should refuse to enter into or continue a correspondent banking relationship with a financial institution 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, financial institutions should not open correspondent accounts with financial institutions that deal with shell banks. Financial institutions should pay particular attention when continuing relationships with respondent financial institutions 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. Financial institutions should establish that their respondent financial institutions 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.

47. Financial institutions 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 30.

ON-GOING MONITORING OF ACCOUNTS AND TRANSACTIONS

48. On-going monitoring is an essential aspect of effective KYC procedures. Financial institutions 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, financial institutions 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, financial institutions 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 financial institutions 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.

49. There should be intensified monitoring for higher risk accounts. Every financial institution 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:

- Financial institutions 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 financial institution .

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

- Financial institutions 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 TRANSACTIONS OR ACTIVITY

50. Where a financial institution suspects, has reasonable grounds to suspect or has information that a transaction or attempted transaction involves proceeds of crime or is related to terrorist financing, 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.

51. Where a financial institutions 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 financial institution 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.

52. If a prescribed entity under Clause 11 of the AMLCTFARO conducts or seek to conduct a transaction through or by using a reporting entity and such transaction or attempted transaction is deemed to be a suspicious transaction involving proceeds of crime or is related to terrorist financing, the financial institution must 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.

53. Where a financial institution 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 financial institution 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.
54. Where a financial institution suspects that a transaction or attempted transaction is unusual, the financial institution 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.

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

56. Section 34 (1) of the AMLCTFA requires financial institutions to each appoint an AML and CTF compliance officer(s) to be responsible for ensuring the company's compliance with the requirements of the AMLCTFA and the AMLCTFARO. The AML and CTF Compliance Officer(s) may be responsible for reporting suspicious transactions or activities to the Director of FlU.

57. 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 financial institution holds the suspicion; and
    (d) be signed or otherwise authenticated by the financial institution.

58. 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.

59. 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.

60. Directors, officers and employees of financial institutions are prohibited from disclosing the fact that an STR or SAR or related information is being reported to the Director of FIU. If financial institutions 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 financial institution 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. Financial institutions should ensure that their employees are aware of any sensitive to these issues when conducting CDD.

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

62. Financial institutions and their employees are protected under Section 43 of the AMLCTFA when complying with their obligations under the Act.

RISK MANAGEMENT

63. 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 financial institution should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the financial institution for ensuring that the financial institution's policies and procedures are managed effectively. The channels for reporting suspicious transactions to the Director of FIU as required under the AMLCTFA should be clearly specified in writing, and communicated to all personnel. Financial institutions should establish internal procedures for assessing whether the financial institution's statutory obligations under the AMLCTFA require the transaction and/or activity to be reported to the Director of FIU. Clause 5 of the AMLCTFARO outlines the appropriate risk-based systems and controls.

64. In accordance with paragraph 30 the AML and CTF compliance officer is responsible for ensuring compliance with the AMLCTFA and the AMLCTFRO.

65. Financial institutions' 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 a financial institution’s compliance function should provide an independent evaluation of the financial institution’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.

66. 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.

67. Section 33 (2) of the AMLCTFA requires that financial institutions have in place an AML and CTF Procedure Manual covering ongoing employee-training programme so that the financial institution employees are adequately trained in KYC procedures. Financial institutions 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.

68. External auditors also have an important role to play in monitoring financial institutions' internal controls and procedures, and in confirming that they are in compliance with supervisory practice. In terms of the FIA and PG 5 - Audit Arrangements, financial institutions' 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

69. The Reserve Bank of Vanuatu has a responsibility to monitor that financial institutions 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 28 of the FIA[12], the Reserve Bank of Vanuatu will be seeking to satisfy itself that appropriate internal controls are in place and that financial institutions 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

70. The Reserve Bank of Vanuatu expects financial institution groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations[13], Parent banks/financial institutions must communicate their policies and

[12] Section 28 of the Financial Institutions Act provides for the Reserve Bank to initiate on-site examinations of the accounts and affairs of any licensee or any of its subsidiaries or affiliates, including any branch, agency or office of the licensee or of its subsidiaries or affiliates. Under Section 28(2) of the Financial Institutions Act, an examination may be conducted by one or more of the following people:
(a) an officer or officers of the Reserve Bank;
(b) any other person or persons appointed by the Reserve Bank as an examiner.

[13] Under Section 41 of the Financial Institutions Act, a domestic licensee requires the prior approval of the Reserve Bank of Vanuatu before establishing a branch, agency or office outside Vanuatu. As part of the review of an application to establish an operation outside Vanuatu consideration would be given to any potential conflict between the KYC policies of a parent bank imposed by the Reserve Bank of Vanuatu and what is permitted in a cross-border

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.

71. 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.

---

office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or the Reserve Bank of Vanuatu, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are.