REPUBLIQUE
DE
VANUATU
JOURNAL OFFICIEL

REPUBLIC
OF
VANUATU
OFFICIAL GAZETTE

6 JUILLET 2009 | EXTRAORDINARY GAZETTE NUMERO SPECIAL NO. 9 | 6 JULY 2009

SONT PUBLIES LES TEXTES SUIVANTS

NOTIFICATION OF PUBLICATION

FINANCIAL INSTITUTION ACT CAP. 254

- PRUDENTIAL GUIDELINE

RESERVE BANK OF VANUATU

THE FINANCIAL INSTITUTION ACT CAP. 254

Pursuant to section 21 (2A) (2B) of the Financial Institution Act, the Reserve Bank has revised prudential guideline No.9 and formulated a new prudential guideline No.12 and hereby issues the following:

1. Bank Supervision Policy Guideline No 9

CUSTOMER DUE DILIGENCE

1. Consistent with ensuring that banks operating in Vanuatu implement sound risk management practices, the Reserve Bank of Vanuatu requires all domestic banks to incorporate the principals and recommendations outlined in this Guideline into their risk management policies. The objective of this guideline is to ensure that 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.

2. In addition to the requirements of this guideline, banks are also expected to comply with the requirements of the Financial Institutions Act No 2 of 1999 and the Financial Transactions Reporting Act [CAP 268] of 2000.

BACKGROUND

3. Internationally supervisors are increasingly recognising 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, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

4. KYC is most closely associated with the fight against money-laundering. The Reserve Bank's approach to KYC is from a wider prudential, not just anti-money laundering or financing of terrorism, 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

5. All banks are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the 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. 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 banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

Customer acceptance policy

6. 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 a 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. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers.

Customer identification

7. 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 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 bank.

8. 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.

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

10. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, 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 a 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.

11. 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 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, 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.

12. 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 a 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. Banks should obtain customer identification papers and retain copies of them

for at least five years after the account is closed. As required under Section 9 of the Financial Transactions Reporting Act, 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 9 of the Financial Transactions Reporting Act also specifies the type of transaction data that must be retained by banks. In line with the requirements outlined in section 9 of the FTR Act 2000, 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 VFIU;
(d) all enquiries relating to the money laundering and the financing of terrorism made to it by the VFIU 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.

13. 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

14. 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.

15. When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the bank should close the account and return the monies to the source from which they were received. It may also be appropriate, if the bank has reasonable grounds to suspect that the account may have been for illegal purposes, for the bank to prepare a Suspicious Transaction Report and submit this report to the Financial Intelligence Unit.

---

[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.

16. Section 9E of the Financial Transactions Reporting Act requires that 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). 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 a bank under section 10 of the FTR Act 2000, the bank should not proceed any further with the transaction unless directed in writing to do so by the FIU and must report the attempted transaction to the FIU as a suspicious transaction.

17. 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, 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 a 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.

18. In terms of section 10H of the Financial Transactions Reporting Act, 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 a bank's compliance function or from supervisory authorities.

SPECIFIC IDENTIFICATION ISSUES

19. Section 10F of the Financial Transactions Reporting Act 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 Part 3 of the Financial Transactions Reporting Act. .

Personal customers

20. For personal customers, 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.

21. Additional information would relate to nationality or country of origin, public or high profile position, etc. Banks should verify the information against original documents of identity issued by an official authority (examples including identity cards, passports and photo driver's license). 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.

22. 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 paragraph 21 above. In such cases banks may rely on other documents (e.g. letters from Chiefs, Pastors, or Magistrates) or other forms of independent identification. In doing so the onus remains on the bank to satisfy itself as to the customer's identity and to ensure that it fully understands the nature of such customers' transactions with the bank.

Corporate and other business customers

23. For corporate and other business customers, 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, 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

24. 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. 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

25. 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. A 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.

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

Introduced business

27. 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, banks may rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, 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. Banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

28. As required under section 10E of the Financial Transactions Reporting Act, 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 this guideline. The ultimate responsibility for knowing customers always lies with the bank. 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 bank would have conducted itself for the customer;

    - The 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 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 bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the Financial Intelligence Unit, where appropriate legal authority has been obtained. In addition, 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

29. When a 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.

30. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks 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 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.

31. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the 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 as the bank. 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 bank should apply the criteria set out in paragraph 27 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

32. Where the intermediary is not empowered to furnish the required information on beneficiaries to the 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 Financial Transactions Reporting Act or anti-money laundering legislation in other jurisdictions, then the bank should not permit the intermediary to open an account.

Politically exposed persons

33. 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.

34. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of Vanuatu's financial system. In addition, a 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, a bank 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 Financial Institutions Act imposes requirements on banks and their officers to satisfy themselves as to the bona fides of the transaction.

35. As required under section 10C (1)(d) of the Financial Transactions Reporting Act, 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. 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.

Non-face-to-face customers

36. 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. 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.

37. 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 banks proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.

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

- 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 bank;
- 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

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

40. Section 10D of the Financial Transactions Reporting Act requires that 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. 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.

41. In particular, 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, banks should not open correspondent accounts with banks that deal with shell banks. 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 anti-money laundering. 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.

42. 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

43. On-going monitoring is an essential aspect of effective KYC procedures. 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, banks are likely to fail in their duty to report suspicious transactions where they are required to do so under the Financial Transactions Reporting Act. The extent of the monitoring needs to be risk-sensitive. For all accounts, 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 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.

44. There should be intensified monitoring for higher risk accounts. Every 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:

- 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 bank.

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

- 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 TRANSACTIONS

1. 45. Where a 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 VFIU. This reporting requirement is outlined in Section 5 of the FTR Act 2000.

2. 46. Section 8(4) of the FTR Act 2000 requires banks to each appoint a compliance officer(s) to be responsible for ensuring the company's compliance with the requirements of the FTR Act 2000. The Compliance Officer(s) would be responsible for reporting suspicious transactions to the VFIU.

3. 47. Section 5E(1) of the FTR Act 2000 states that a suspicious transaction report 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.

4. 48. A suspicious transaction report may be given orally, including by telephone, but a written report must be prepared in accordance with section 5E(1) within 24 hours after the oral report is given.

5. 49. Compliance Officers should keep a register of all reports made to the VFIU and all reports made internally to them by employees.

6. 50. Directors, officers and employees of banks are prohibited from disclosing the fact that an STR or related information is being reported to the VFIU. If 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 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. Banks should ensure that their employees are aware of any sensitive to these issues when conducting CDD.

7. 51. If satisfactory evidence is not produced to or obtained by a bank under section 10 of the FTR Act 2000, the bank should not proceed any further with the transaction unless directed in writing to do so by the FIU and must report the attempted transaction to the FIU as a suspicious transaction.

52. Banks and their employees are protected under Section 17 of the FTR Act 2000 when complying with their obligations under the FTR Act.

RISK MANAGEMENT

53. 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 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 bank for ensuring that the bank's policies and procedures are managed effectively. The channels for reporting suspicious transactions to the Financial Intelligence Unit as required under the Financial Transactions Reporting Act should be clearly specified in writing, and communicated to all personnel. Banks should establish internal procedures for assessing whether the bank's statutory obligations under the Financial Transactions Reporting Act require the transaction to be reported to the Financial Intelligence Unit.

54. Section 8(3) of the Financial Transactions Reporting Act requires that banks appoint a compliance officer who is responsible for ensuring compliance with the Act and establish an audit function to test its anti-money laundering and financing of terrorism procedures and systems.

55. 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 a bank's compliance function should provide an independent evaluation of the 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.

56. 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.

57. Section 8(1) of the Financial Transactions Reporting Act requires that banks have an ongoing employee-training programme so that bank employees are adequately trained in KYC procedures. 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.

58. External auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice. In terms of the Financial Institutions

Act and Prudential Guideline 5 – Audit Arrangements, 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

59. The Reserve Bank of Vanuatu has a responsibility to monitor that 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 28 of the Financial Institutions Act[2], the Reserve Bank of Vanuatu will be seeking to satisfy itself that appropriate internal controls are in place and that 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

60. 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[3]. 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

---

[2] 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.

[3] 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 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.

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.

61. 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.

2 Prudential Guideline No 12

OPERATIONAL RISK MANAGEMENT

8. This Guideline outlines a set of principles that provide a framework for the effective management of operational risk by banks. In this guideline, operational risk is defined and recommendations are outlined on the basis of the standards contained in the paper issued by the Basel Committee on Banking Supervision in February 2003, titled *Sound Practices for the Management and Supervision of Operational Risk.*

9. The requirements established in these Guidelines constitute general requirements which a bank shall take into account in the arrangement of operational risk management conforming to the needs and options of the organization. The scope of application of the Guidelines depends on the organizational structure and culture, business volume and risk level of a bank, as well as on the legal complexity of the financial services and products offered by, and the characteristic features of risk management and accounting system of, the bank.

10. This guideline should be read in conjunction with the Financial Institutions Act 1999. The adoption and implementation of sound risk management practices re-assures a bank's depositors and engenders confidence in a bank.

BACKGROUND

11. Deregulation and globalization of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their risk profiles (i.e. the level of risk across a firm's activities and/or risk categories) more complex. Developing banking practices suggest that risks other than credit, interest rate and market risk can be substantial.

12. Operational risk is a term that has a variety of meanings within the banking industry, and therefore for internal purposes, banks may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear

understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing the bank and captures the most significant causes of severe operational losses.

13. Operational risk event types having the potential to result in substantial losses include:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.

- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.

- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.

- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.

- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.

- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty miss-performance, and vendor disputes.

14. The diverse set of risks listed above can be grouped under the heading of 'operational risk', which the Basel Committee has defined as *'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'*. The definition includes legal risk but excludes strategic and reputational risk.

OPERATIONAL RISK MANAGEMENT

Identification of operational risk

15. Operational risk is a distinct risk area. Each bank shall formulate a definition of operational risk for its internal use. The definition of operational

risk shall be based upon the scope and complexity of the business and previous experiences in the risk management of the bank and shall clearly articulate the factors that may cause an operational risk in the bank.

16. The content of a definition of operational risk shall commensurate with the business practices of a bank (IT solutions used and complexity thereof; outsourcing, personnel policy, complexity of risk management relating to services and products offered; external insurance, etc.).

Arrangement of operational risk management

17. Operational risk management is a distinct risk management area. Operational risk management shall constitute an integrated part of the corporate governance and the general risk management system of a bank. Operational risk management shall be accompanied by improved definition and positioning of the activities of a bank, and transition from defensive activities to activities that involve the analysis of risks and prevention of loss events.

18. In the arrangement of operational risk management a bank should take into account that operational risk losses are not always measurable and they may be incurred after a substantial amount of time and/or indirectly.

19. Operational risk management is a process that requires a uniform understanding of operational risk organization-wide and it is based upon high organizational culture along with the relevant risk culture and positive attitude toward internal control. In operational risk management, the creation of unfounded "feeling of security" must be avoided, as this may entail the establishment of inappropriate objectives and unintended results (first of all as regards business continuity management).

20. In the application of these Guidelines, a bank shall seek to find a solution that is optimal and economically reasonable for its, while being in line with the scope of its business and comprising all legal and business units of the organizational structure. In the implementation of the requirements established in the Guidelines in the different units of a bank, excessive bureaucracy shall be avoided and the assumptions of efficiency of operational risk management and the value added created thereby shall be taken as the basis.

21. The understanding of a bank of the operational risks inherent in its business and the willingness to pay attention to operational risk management besides conventional risk management systems and means (analysis models and programs, stress tests, etc.) are of essence.

22. The activities of a bank which relate to operational risk management should be subject to independent review and assessment.

DUTIES OF THE BOARD AND SENIOR MANAGEMENT

Duties of the Board

23. The duties of the Board include establishing the organizational, business and risk management structure which is appropriate for operational risk management, as well as general principles of supervising the activities of the bank.

24. Where the volume and scope of the business of a bank render it unreasonable to ensure the segregation of business and control structures, ways of risk mitigation by means of other measures shall be sought (e.g. additional controls, reporting, the so-called four-eye principle, etc.).

25. It is the duty of the Board to ensure the creation of an internal control environment that supports efficient operational risk management involving all the units and activities of the bank. For foreign banks, the policy statement should be approved by an appropriate senior officer from outside of Vanuatu.

26. The Board shall establish the definition of operational risk and the general principles (policy) of risk management and revise the same on a regular basis, taking into account, inter alia, changes in the activities and operating environment of the bank.

27. The Board shall, in conjunction with senior management, allocate the resources that are necessary for continuous development and implementation of operational risk management (budgetary resources, motivated employees with relevant qualifications).

28. The Board shall be aware and have a clear understanding of the major operational risks inherent in the organization (IT, personnel), areas of activity and operating environment of the bank. The Board shall be provided with regular reports and overviews concerning the operational risk position of the bank, the circumstances that have caused changes in that position and, operational loss events.

29. The Board shall ensure the capability of the bank's internal audit function (qualified and motivated employees) to assess the internal regulations and activities that relate to operational risk management. The scope of activities of the internal audit function shall be sufficient to obtain assurance about the adequacy and efficiency of operational risk management.

30. While the internal audit function should not be directly responsible for particular activities relating to operational risk management, an optimal and economically reasonable solution should be found in conjunction with the risk management units, which corresponds to the bank's scope of activity and nature of risks.

Duties of Senior Management

31. Senior management shall design the organizational structure so as to ensure that areas of responsibility, reporting relationships and procedures of structural units are clearly identified. The segregation of the lines of accountability and reporting of the bank's business and control structures shall be ensured.

32. It is the duty of senior management to introduce routines in the bank which are based on sound risk management practices (the segregation of functions, the so-called four-eye principle, etc.), see to it that the routines are adhered to, and ensure the operation of the internal control environment, using regular reports and engaging the internal audit, if appropriate.

33. Senior management shall be responsible for the implementation of the operational risk management principles (policy) approved by the Board within the bank. The operational risk management policy shall be implemented throughout the bank and all the levels of staff should understand their responsibilities with respect to operational risk management and ensure the performance of the related obligations.

34. Senior management shall be responsible for the development of sub-policies and internal regulations for management of operational risks inherent in all products, activities, processes and systems. While the manager of each structural unit is responsible for the appropriateness and efficiency of the operational risk management principles and internal regulations within his or her purview, the senior management shall clearly determine the authority, liability and procedure for reporting in order to maintain that accountability.

35. Senior management shall ensure that the operational risk management policy and the internal regulations for implementation thereof are communicated to all employees in all structural units that are exposed to operational risk. Employees' clear understanding of the risk management-related rights and obligations arising from their positions shall be ensured.

36. Senior management shall see to it that day-to-day activities relating to operational risk management are performed by qualified staff with sufficient experience and technical capabilities necessary for the work.

37. Employees responsible for monitoring and implementation of risk management in the bank shall have authority independent of the structural units and activities they oversee.

38. Employees responsible for operational risk management shall consistently exchange information with employees responsible for credit, market and other risks.

39. Senior management shall implement a remuneration policy within the bank (wages, extra pays, benefits, etc.), which is consistent with the risk profile of the bank and supports sound risk management practices and the internal control environment.

OPERATIONAL RISK POLICY

40. The aim of operational risk policy is to render the definition of the risk and ascertain the methods and means of identification, measurement, monitoring, mitigation and control of the risk.

41. Operational risk policy shall underlie the management of all the activities of the bank that relate to operational risks. The content of that policy shall commensurate with the scope and volume of the bank's business and cover all operational risks inherent in the activities of the bank.

42. Operational risk policy shall contain references to areas relevant to operational risk management. These areas include, among others, physical security of the bank, manageability of IT systems, data protection, business continuity, prevention of money-laundering, personnel policy, etc.

43. Depending on the scope and volume of the bank's business and the nature of the services and products offered by it, the operational risk policy shall identify the activities the purpose or contents of which have a direct or indirect impact on the bank's activities in operational risk management. Such activities include, e.g., the development of new products and services, the selection of external service providers, development activities (incl. IT), etc.

IDENTIFICATION AND ASSESSMENT OF OPERATIONAL RISKS

44. The identification and classification of operational risks shall be based on a bank-wide understanding of operational loss events. A clear identification of loss events enables a bank to distinguish operational risk from credit and market risks and to quantitatively assess the operational risk.

45. A bank shall identify and assess the operational risks inherent in all of its products, activities, processes and systems. A bank shall also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risks inherent in them are subject to adequate assessment procedures.

46. Effective risk identification considers both internal factors (such as the complexity of the organizational structure, the nature of the bank's activities, qualification of personnel, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

47. In addition to identifying the operational risks, a bank shall also assess its vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

48. Examples of processes/activities used for identifying operational risks include:

a) **Risk mapping**: in this process, various sub-units or owners of business or auxiliary processes of an organization map the risks inherent in their units/businesses/processes by risk type.
b) **Risk assessment**: in this process, various sub-units or owners of business or auxiliary processes of the bank analyze the probability of occurrence and financial impact of a risk event (using the help of risk management staff and/or external consultants, if appropriate).
c) **Key risk indicators**: risk indicators are statistics and/or metrics (measurements), often financial, which can provide insight into the risk position of a bank. These indicators are usually reviewed on a periodic basis (such as monthly or quarterly) in order to be aware of changes that may be indicative of risk concerns. Such indicators may include the number of failed transactions, staff turnover rates and the frequency and/or severity of errors and omissions.
d) **Monitoring of thresholds/limits relating to risk indicators**: exceeding these thresholds/limits alerts the management to the existence of spheres with potential inherent problems.

49. Data on a bank's historical loss experience could provide information for assessing the bank's exposure to operational risk. An effective way of collecting and making good use of this information is to establish a classification for systematically tracking and recording the frequency, severity and other relevant information on individual loss events.

50. It would be reasonable to use the classification developed by the Basel Committee on Banking Supervision as the basis for the classification system. The classification system may differ across banks, but it should, as a general rule, comprise the following types of loss events:

a) internal fraud;
b) external fraud;
c) employment practices and workplace safety;
d) customers, products and business practices;
e) damage to physical assets;
f) business disruption and system failures;
g) execution, delivery and process management.

51. The inclusion of operational loss events in individual classes in pursuance of the general nature of the operational loss events allows a bank to assess the risk mitigation measures employed for reducing the probability of occurrence

and impact of those events. The system of classification of loss events should enable a bank to determine the types of events that might potentially result in material damage and provide direct information on the need for use, and the effectiveness and efficiency, of risk management measures.

52. In addition to the classification of operational risks by types of loss events, a bank should also classify loss events by types of principal fields of business. The fields of business underlying such classification may differ across companies.

53. Information about loss events principally comprises usual, high-frequency, low-severity events and low-frequency high-severity events. It would be reasonable to establish a reporting system that allows tracking and recording both types of loss events, including external information about material loss events.

54. High-severity events in a bank are generally accompanied by an improvement of the control system of the relevant sphere or activity (or the spheres or activities corresponding to the same criteria in the whole of the bank), which should substantially reduce the probability of occurrence of similar loss events in the future. In order to achieve a control environment that contributes to the prevention of loss events, it is important to take notice of high-severity loss events that have occurred in banks similar to the bank in question, and of the conditions and circumstances of occurrence of these loss events. This contributes to assessment of the probability of occurrence of similar loss events and testing the operation of the bank's control environment and to material reduction of the probability of occurrence and/or financial impact of the loss events.

OPERATIONAL RISK MONITORING

55. An effective monitoring process is essential for ensuring adequate operational risk management. Regular monitoring of activities offers the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk, and preventing losses.

56. In addition to monitoring operational loss events, a bank shall identify and monitor the indicators that provide early warning of an increased risk of future losses. Such risk indicators (key risk indicators) should be forward-looking and reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, interruptions in transactions and activities, system downtime, etc. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon the (growing) risks appropriately.

57. Risk indicators may derive from the particular lines of business or comprise all of the areas of activity or units of a bank. Examples of such indicators include:

a) the number of customer complaints;
b) the number of customer compensation events;
c) the number of interrupted transfers and transactions;
d) employee turnover;
e) the number of observations / precepts by supervisory authorities;
f) the number of failures, or manageability, of (IT) systems;
g) the number of internal policies and procedures in need of amendment.

58. Monitoring is the most efficient if the control system is an integral part of the activities of a bank and if the relevant regular reporting is stipulated. In addition to the reports to be submitted to the manager of the sphere in question, the results of such monitoring should be reflected in the reports submitted to senior management and the Board, as well. The contents of reports drawn up by the supervisory function may also serve as input for the monitoring.

59. Senior management and the Board shall receive regular reports from both business units and the internal audit unit (and the reports should be distributed to all the appropriate levels of management). The reports should contain internal financial, operational, and compliance data and fully reflect any identified problem areas and should motivate timely corrective measures.

60. To ensure the usefulness and reliability of these risks and audit reports, management should regularly verify the timeliness, accuracy and relevance of reporting systems and internal controls in general, using reports prepared by external sources (auditors, supervisors) to that end. Reports shall be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

CONTROL AND MITIGATION OF OPERATIONAL RISK

61. A bank shall have policies, processes and procedures in place to control and mitigate material operational risks. A bank shall review the appropriateness of alternative risk limitation and control strategies and should adjust its operational risk profile accordingly using appropriate strategies, in light of their overall risk tolerance and profile of the bank.

62. Control activities shall be in place which are designed to address the operational risks that a bank has identified. For the risks that can be controlled, a bank should decide to which extent to use control activities and other appropriate measures, and to which extent to accept these risks. For those risks that cannot be controlled, a bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

63. A bank shall establish and implement control activities and procedures for ensuring compliance with the established set of internal policies concerning the risk management system. Principle elements of this could include, for example:

a) top-level reviews of the bank's progress toward the stated objectives;

b) a system of documented approvals and authorizations to ensure that activities are carried out at an appropriate level of management;
c) policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues.

64. Although a system of formal, written policies and procedures is critical, control activities need to be carried out through a strong internal control function. To ensure efficiency, control activities should be an integral part of the regular activities of a bank, which makes it possible to quickly respond to changing conditions and avoid unnecessary costs.

65. An effective internal control environment requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to employees or to sub-units of the bank may enable them to cause losses or errors or carry out inappropriate actions. Therefore, potential conflicts of interest shall be identified, minimized and be subject to independent monitoring and review. The relevant data should be included in risk reports.

66. In addition to segregation of duties, a bank shall ensure that other internal measures are in place as appropriate to control operational risk, such as close monitoring of adherence to assigned risk limits or thresholds; control of access to, and use of, assets and documents (ensuring security); ensuring that staff have appropriate expertise and training; identifying business lines or products where returns materially differ from expectations; and regular verification and reconciliation of transactions and accounts.

67. Operational risk can be more pronounced where a bank engages in new activities or develops new products (particularly where these activities or products are not consistent with the bank's core business strategies) or has entered unfamiliar markets. Owing to business objectives and customary preference thereof, there is a risk that a bank cannot ensure that its risk management infrastructure keeps pace with the growth in the business activity. Therefore, it is crucial in such a situation to ensure that special attention is paid to the development and operation of internal control functions.

68. Some significant operational risks have low probabilities but a potentially very large financial impact. While a bank cannot control all risk events (e.g., natural disasters), risk mitigation tools or activities can be used to reduce the frequency and/or severity of such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalize the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims arising from errors or omissions, employee or third-party fraud, and natural disasters, etc.

69. A bank should view risk mitigation tools (incl. insurance policies) as complementary to, rather than a replacement for, internal operational risk control. Consideration also needs to be given to the extent to which risk

mitigation tools truly reduce risk, or transfer the risk to another business area, or even create a new risk.

70. Investments in banking technology and information technology security are important for operational risk mitigation. Attention should be paid to the circumstance that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with an interruption or extended disruption of business caused by internal or external factors. A bank should establish business continuity plans that address this risk.

OUTSOURCING[4]

71. A bank should establish a policy for managing risks associated with outsourcing activities and determine the terms and conditions of selection of external service providers and of entry into contracts with them.

72. In the selection of external service providers, a bank should assess, among other things, the following:

a) impacts (financial, reputation, business continuity, etc.), if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
b) potential loss or damage to be incurred by the bank and other parties/persons, if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
c) the ability to comply with supervisory and regulatory requirements (taking into account possible changes in these requirements);
d) the consumption of financial resources and time in the case of a need to replace a service provider or reinstate the provision of the service in the responsibility of the bank (business continuity management);
e) the need for, and the terms and conditions of, carrying out due diligence of the service provider, and ensuring business continuity management;
f) issues relating to the ownership right in physical and intellectual property (e.g. hardware and software, licenses, documentation concerning systems and processes).

73. Outsourcing arrangements should be based on contracts containing explicit terms and conditions that ensure a clear allocation of rights, obligations and responsibilities between external service providers and the outsourcing bank. The rights and obligations of the parties to such a contract should be clearly defined, understandable and applicable. The terms and conditions of the contract should, as a general rule, contain the following:

---

[4] Outsourcing means the assignment of certain activities necessary for carrying out the day-to-day business of a bank (e.g. development and management of information technology, cash management, administrating activities, personnel management, real estate management, transportation) to third persons.

a) the exact contents of the services to be provided, and the requirements established with regard to the volume and quality of the services;
b) the right of the bank to have access to essential information concerning the services to be provided (related contracts, accounting information, etc.);
c) confidentiality of information (incl. information concerning customers);
d) the procedure for resolution of dissension and disputes;
e) rights and obligations relating to suspension or termination of the contract.

74. The use of an external service provider shall not reduce the capability of a bank to carry out its regular activities and comply with obligations to customers, third parties and supervisory authorities.

75. Outsourcing activities can reduce the risks of a bank by transferring certain activities to persons with greater expertise and opportunities to carry out these activities and to manage the risks associated with the activities. However, the use of external service providers does not diminish the responsibility of the Board or senior management of a bank to ensure that the outsourced services are provided in a safe manner (incl. the protection of customer data) and in compliance with applicable laws.

BUSINESS CONTINUITY MANAGEMENT[5]

76. For reasons that may be beyond the control of a bank, circumstances can occur that result in the inability of the bank to fulfill some or all of its business obligations (incl. liquidity), particularly where the bank's physical (office(s), staff), telecommunications, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. Therefore, a bank shall establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

77. With a view to the implementation of the disaster recovery and business continuity plan, a bank should, among other things:

a) appoint persons participating in crisis management and business resumption;
b) carry out relevant training programs, incl. communication with the media and public at large;

[5] Business continuity management comprises activities that are designed to improve the ability of a bank to respond to business interruptions and to restore its key activities, systems and process within an agreed period of time, while maintaining the critical activities of the bank.

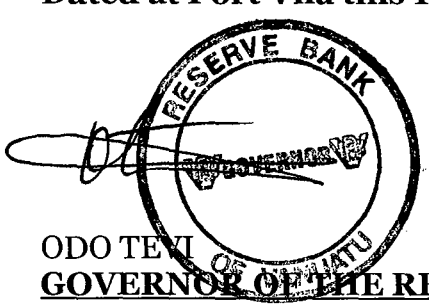
c) create and supply crisis management centres;
d) enter into preliminary agreements with possible internal and external persons and external service providers;
e) create alternative options for recording and backing up electronic data;
f) introduce the plan within the bank and carry out awareness/readiness checks;
g) prepare communication with all interested parties.

78. Particular attention should be paid to the ability to restore the electronic data that are necessary for business resumption. Where the copies of such data are maintained at an off-site facility, or where the operations of a bank must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimize the risk that both original and back-up data and both primary and back-up facilities will be unavailable simultaneously.

79. A bank should periodically review its disaster recovery and business continuity plan to ensure that it is consistent with the bank's current operations and business strategies. Moreover, such a plan should be tested periodically to ensure that the bank is able to execute the plan in the actual event of a business disruption.

3. This notice will be effected as of the date of the gazette.

Dated at Port Vila this 10th day of June 2009



ODO TEVI
GOVERNOR OF THE RESERVE BANK