ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML AND CTF) PROGRAM
PART A

1. AML and CTF Risk Assessment

1.1. This AML & CTF Program sets risk assessment process which is grounded on risk-based approach.

1.2. The main components of the risk assessment process are:

1.2.1. Risk identification,

1.2.2. Management and mitigation of risks, and

1.2.3. Risk assessment reporting.

1.3. In identifying ML/TF risks, PPB has considered the risk posed by the following risk factors:

1.3.1. our customer types, including any Politically Exposed Persons;

1.3.2. the types of services we provide;

1.3.3. the methods by which we deliver our services;

1.3.4. the foreign jurisdictions with which we deal; and

1.3.5. the business structure and process.

1.4. The risk assessment will provide the foundation for

1.4.1. The categorization of customers into different due diligence levels within the KYC process, and

1.4.2. The identification of situations and cases where monitoring and/or other additional risk mitigation measures will be required.

2. Risk Factors Considered

For the purposes of the AML and CTF Act, in identifying its ML/TF risks, PPB has considered the risks posed by the five factors listed in paragraph 3.3 above and set out in detail below. Thus, certain customer types, services, delivery methods, foreign jurisdiction considerations and business structures and processes can pose a higher ML/TF risk.

At a high-level, risk factors that we may reasonably face are identified as follows:

2.1. **Customer Type:**

2.1.1. The customer identity, origin of wealth or source of funds cannot be easily verified;

2.1.2. Where the structure of the customer/entity renders it difficult to identify the true controlling owner, or where there is no legitimate commercial rationale for the structure;

2.1.3. The customer is a Politically Exposed Persons (“PEP”);

2.1.4. Customers engaged in a business which involves the physical handling of significant amounts of cash (e.g. currency exchange bureau, money transmitters, dealers in high value goods, on-line auction sites, casinos,

betting and other gambling related activities who routinely receive payment in cash);

2.1.5. Customers who appear on governments lists, including sanction lists, or other credible sources which trigger risks in respect of corruption and/or criminal activity;

2.1.6. Customers (not necessarily PEPs) based in, or conducting business in or through, a high risk geographic location, or a geographic location with known higher levels of corruption or organized crime, or drug production/distribution;

2.1.7. Charities and other "not for profit" organizations which are not subject to some form of regulatory monitoring or supervision.

2.1.8. Professional service providers such as lawyers, accountants, investment brokers or other professionals holding accounts for their customers or acting on behalf of their customer and where we would be required to place an unreasonable reliance on the professional service provider;

2.1.9. Requests for undue levels of secrecy with a transaction;

2.1.10. Whether the customer is a long-standing customer or undertakes occasional transactions;

2.1.11. The customer's business activities place the customer in a high risk category (military industry, casino etc.)

2.2. The Types of Services Provided

PPB is a company structured to provide private banking, asset management and wealth management services to retail and wholesale clients. Although not necessary, certain products, services and transactions in relation to them may pose a higher risk. E.g. the following products and services may pose a high risk under certain circumstances:

2.2.1. Services where large amounts are invested;

2.2.2. Services involving structures intended to (or which can in practice) render a customer anonymous (e.g. accounts in the names of trusts or nominees of third persons);

2.2.3. Third-party accounts/client accounts/pooled accounts;

2.2.4. Correspondent banking services.

2.3. The methods by which we deliver our services

Products and services provided in a non - face to face process, i.e. when the customer has not been physically present for identification purposes may pose higher risks.

2.4. Foreign Jurisdictions

Customers based in, or conducting business through certain countries may pose a higher risk. Criteria for identifying high risk countries are e.g.:

2.4.1. Countries identified by credible sources as providing funding or support for terrorist activities or who have terrorist groups working within the country;

2.4.2. Countries subject to sanctions and embargoes by the United Nations;

2.4.3. Countries identified by credible sources as having significant levels of corruption and/or criminal activity;

2.4.4. Countries identified by credible sources as lacking appropriate AML and CTF legislation;

2.4.5. Countries identified by the FATF as non-co-operative countries and territories.

For a updated list of High risk jurisdictions please refer to Annex 5.

2.5. **Business Structure and Process**

PPB's simple organizational and business structure as well as clearly defined business and operational processes allow to define AML and CTF risk according this criteria as low.

3. Management and mitigation of risks

3.1. Based on the risk assessment foundation, the following measures shall be applied:

3.1.1. Assigning risk level (low, medium or high) to all customers, based on the risk assessment foundation,
3.1.2. Applying enhanced due diligence measures to high risk customers,
3.1.3. Increasing staff awareness and knowledge of AML and CTF and PPB's measures to prevent it (e.g. through frequent/deeper staff training),
3.1.4. Monitoring of customers' activities and transactions, carried out manually by the client relationship manager within ongoing customer due diligence, and electronically by AML and CTF Compliance Officer (s)[1],

[1] Available after launch of the new core banking system with AML alert functionality. Expected to go live in September 2015.

3.1.5. Escalating the decision regarding establishment of a relationship in the case of an high risk customer, or (where appropriate) carrying out of a specific action, including procedures for the rejection or termination of customer relationships, and

3.1.6. Reviewing and amending AML and CTF processes and routines.

3.2. Whenever a certain risk is identified that needs mitigation, risk mitigation measures shall be considered and implemented in relation to each of new and existing customers, and new and existing products and services. If the identified risks cannot be mitigated immediately, an action plan shall be established.

4. Compliance function in AML and CTF

4.1. PPB has established compliance function within the bank directly reporting to the Board of Directors, led by General Counsel and Chief Compliance Officer and having specifically dedicated staff as AML&CTF Compliance Officers.

4.2. Responsibilities of AML and CTF Compliance Officer (s):

4.2.1. monitoring compliance and adherence to the obligations of the AML and CTF Act;

4.2.2. receiving and investigating reports of suspicious matters activities;

4.2.3. adopting a risk based approach to monitoring customer activity to identify suspicious activity;

4.2.4. ensuring that proper AML and CTF records are maintained;

4.2.5. reporting suspicious activity to FIU;

4.2.6. providing advice to Representatives;

4.2.7. receiving and carrying out directions or orders issued by General Counsel and Chief Compliance Officer and/or Authorities; and

4.2.8. liaison with Reserve Bank Vanuatu, FIU, other regulatory bodies and law enforcement in respect of suspicious activity reporting and threshold reporting.

4.3. AML and CTF related responsibilities of General Counsel and Chief Compliance Officer (s):

4.3.1. preparation and review of AML Policy and Program;

4.3.2. overseeing communication and training for employees;

4.3.3. providing advice to AML&CTF Compliance Officers and other Representatives;

4.3.4. submitting reports to the Board (at least annually);

4.3.5. lodging annual compliance report with Authorities;

4.3.6. receiving and carrying out directions or orders issued by Authorities; and

4.3.7. liaison with Reserve Bank Vanuatu, FIU and other regulatory bodies and law enforcement in respect of suspicious activity reporting and threshold reporting.

4.4. General Counsel and Chief Compliance Officer as well as AML and CTF Compliance Officer (s) are authorised and have full capacity to act independently in order to fulfil the commitments of his/her role as well as receive all information necessary to carry out the compliance functions from the Representatives.

4.5. The compliance function must be consulted prior to PPB: introducing a new designated service to the market; introducing new methods of delivery of a designated service; and/or introducing any new or developing technology used for the provision of designated services to enable the AML and CTF Compliance Officer (s) to identify any significant changes in ML/TF risks and to formulate controls to mitigate and manage those risks.

5. Risk assessment reporting

5.1. It is the responsibility of AML&CTF Compliance Officers to report suspicious activity or transactions and file incident reports to the Authorities as well as keep the General Counsel and Chief Compliance Officer informed on the everyday basis about all AML and CTF issues, defaults or incidents.

5.2. General Counsel and Chief Compliance Officer shall, on an ongoing basis, inform the Managing Director and the Board of Directors of the material events related to management and mitigation of Money Laundering risks in PPB.

5.3. The relevant reported AML and CTF related information is included in an annual compliance report prepared by the General Counsel and Chief Compliance Officer and presented to the Board of Directors. The report shall contain information on incidents and/or outlined areas that need improvement and where there are deficiencies or proposals for improvement, a plan showing how these are to be handled.

5.4. Records shall be kept of all reports in accordance with general record keeping principles.

6. AML and CTF Training Program

6.1. Appropriate training with regard to money laundering and terrorist financing is vital in managing the ML/TF risk. Accordingly, all Representatives of PPB are required to undergo training in AML and CTF laws and PPB's internal policies. In order for our ML/TF controls to be successful, training programs are formulated having regard to the representative's level of responsibility and position.

6.2. Updated or refresher training will depend upon staff promotions and/or depending upon the level of assessed ML/TF risk of the designated service.

6.3. The training can be internal or external (by contracted training organisations). Specific AML and CTF related external training would be available to certain Representatives according their responsibilities (such as General Counsel and Chief Compliance Officer, AML/CTF Compliance Officers etc.). It is a responsibility of General Counsel and Chief Compliance Officer to arrange internal training. Ongoing training will occur on a periodic basis.

6.4. At a minimum the AML and CTF training program will be designed to enable Representatives to understand the following:

6.4.1. the AML and CTF Policy;

6.4.2. the AML and CTF Program;

6.4.3. the obligations of PPB under the AML and CTF Act and underlying legal requirements;

6.4.4. the types of ML/TF risk PPB might face and the potential consequences of such risks;

6.4.5. how to identify signs of ML/TF that arise during the course of carrying out their duties;

6.4.6. escalation procedures i.e. what to do once a ML/TF risk is identified;

6.4.7. what employees' roles are in the firm's compliance efforts and how to perform them i.e. the processes and procedures relevant to each person's role;

6.4.8. the company's record keeping and record retention policy; and

6.4.9. the consequences (including civil and criminal penalties) for non-compliance with the AML and CTF Act and supporting Rules.

6.5. Records of training must be maintained to demonstrate that the person/s attended the training session/s, the dates of training, a brief description of the subject matter of the training provided and the number of hours (or level of accreditation) for attending the course/session/seminar.

6.6. Training frequency:

6.6.1. Annually: All employees dealing with client-related matters or, who, due to the nature of their position, have special needs of AML knowledge, shall undergo training, be updated and/or informed regarding important and relevant AML regulations and relevant internal procedures as appropriate. All newly on boarded Representatives shall undergo training within 3 (three) months.

6.6.2. Ongoing: For employees operating in areas which may represent high risk, e.g. correspondent banking, the need for tailor made training or information shall continuously be assessed by General Counsel and Chief Compliance Officer in collaboration with the business, and when a need is identified, action shall be taken.

7. Monitoring process and Suspicious Matter Reporting

7.1. PPB has implemented Transaction Monitoring process defined herein which includes appropriate risk-based systems and controls to scrutinize transactions that are inconsistent with information held about the business relationship with the reporting entity. The transaction monitoring system is set to identify any transaction that appears to be suspicious, complex, unusual and have no apparent visible economic or lawful purpose;

7.2. PPB has also implemented Customer Monitoring Process where it monitors its relationship with its customer ensuring that the customer's activities being conducted are consistent with PPB's knowledge of the customer, the customer's business, source of funds and risk profile;

7.3. Customer activities and transactions shall, based on a risk based approach, be monitored by the client relationship manager within day to day activities and within ongoing customer due diligence and electronically by AML and CTF compliance officer (s)[2]. Any and every payment that wouldn't fall within the expected payments associated with certain clients should be singled out and further examined by the AML/CTF Compliance Officers.

7.4. All monetary transactions and related data (accounts, involved parties and relations) are to be individually and manually reviewed and their purpose verified by the document substantiating the purpose of the transaction (contracts, invoices, loan agreement etc.). This requirement may be exempted in cases of small amount transactions or otherwise due to risk based approach applied in the Bank. Furthermore, every incoming and outgoing payment has to be filtered through the World Check's sanctions lists and/or any other reliable sources available to the Representative at the moment.

7.5. The initial or ongoing due diligence and monitoring may give rise to concerns requiring a review. The following are examples of circumstances which may give rise to such concerns:

7.5.1. Refusal to disclose details concerning business activities, e.g. unwillingness to disclose the source of funds or wealth or unwillingness

[2] Available after launch of the new Core banking system with AML alert functionality. Expected to go live in September 2015.

to provide names of and other information on owners and other people with significant control over the business entity,

7.5.2. The behavior of the customer diverges from previous pattern or stated pattern, e.g. an inactive account suddenly becomes active with large transactions,

7.5.3. A prospective customer promises a trading volume, which does not make economic sense in the light of his background and other activities,

7.5.4. The purpose and intent behind the transaction or relationship is unclear, e.g. when the commercial rationale for certain service is missing or weak,

7.5.5. The representative suspects on reasonable grounds that the customer is not the person they claim to be or that the customers agent is not the person they claim to be,

7.5.6. The Representative suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of financing of terrorism.

7.6. The assessment as to what constitutes suspicion shall be based on the information about the client received by the Representative handling the matter, and the scope of the client's business, along with the Representatives general knowledge of deviating or suspicious transaction or activity patterns.

7.7. If the result of a review gives rise to an actual or potential suspicion related to Money Laundering the Representative shall immediately report the issue to compliance function, which shall initiate an investigation and decide whether to report the issue to the FIU. Matters of a more serious nature where a report to FIU has been filed shall be reported to the Board of Directors.

7.8. AML/CTF Compliance Officer (s) are responsible for the reporting to FIU.

7.9. Detailed suspicious matter reporting requirements are set in AML&CTF Act Part 6 and include:

7.9.1. obligation to report suspicious transaction (STR);

7.9.2. obligation to report suspicious activity (SAR);

7.9.3. obligation to report transaction conducted by prescribed entities (as defined in AML&CTF Act Rules Article 11);

7.9.4. obligation to report transaction involving terrorist property;

7.9.5. obligation to report certain transaction with no legitimate purpose;

7.9.6. other reporting obligations which may or may not be connected with suspicions in ML/TF activities, and include obligation to report international currency transfers (above 1000000 VT or equivalent in foreign currency), obligation to report large cash transactions (not applicable to PPB since no cash transactions are allowed).

7.10. The procedure for suspicious matter reporting is described in Annex 9 Suspicious matter reporting.

7.11. Suspicious Transaction Report (**STR**) is to be filed **on a transaction** or attempted transaction regarding which PPB suspects or has reasonable grounds to suspect that it involves proceeds of a crime, relate to terrorist financing, is complex, unusual or large, and does not have any apparent visible economic or lawful purpose.

7.12. In slight contrast a Suspicious Activity Report (**SAR**) shall be reported on a **series of transactions** and/or attempted transactions (which form a pattern or trend) which PPB suspects or has reasonable grounds to suspect to involve proceeds of crime or is related to terrorist financing.

7.13. It is important that any attempt to overcome the threshold requirements by conducting 2 or more transactions below the prescribed threshold amounts with the purpose to avoid the reporting has been identified, investigated and where necessary reported to the authorities.

7.14. Reports filed with FIU on suspicious Money Laundering or financing of terrorism shall be recorded and kept according requirements set out in this Program.

7.15. It is prohibited to disclose to the customer concerned or to other third persons outside PPB the fact that a report has been filed or that a Money Laundering investigation is being or may be carried out.

7.16. PPB must take all appropriate measures to protect Representatives who report suspicious activity from being exposed to threats or hostile action.

8. Record Keeping

8.1. In accordance with meeting legislative obligations, PPB will retain all records relevant to its AML and CTF Program and policies, including the following:

8.1.1. the AML and CTF Program and all reviews and addendums to the same;

8.1.2. its AML and CTF Policy and all reviews and addendums to the same;

8.1.3. transactional records;

8.1.4. Customer identification and verification records;

8.1.5. Audits and compliance reviews;

8.1.6. Suspicious matter and other reports made to FIU;

8.1.7. All enquiries relating to ML and TF made to PPB by the FIU or law enforcement agency;

8.1.8. Management approvals;

8.1.9. Customer account/relationship records;

8.1.10. Annual compliance reports and other management reports;

8.1.11. Training and compliance monitoring reports; and

8.1.12. Information relating to the effectiveness of training.

8.2. Records in respect of customer identification and verification are to be retained for 6 years after account closure.

8.3. Where PPB (or its agent or intermediary) carries out a customer identification and verification procedure with respect to a prospective customer to whom PPB proposes to provide a service, it must make (and retain) a record of:

8.3.1. the procedure (i.e. the Checklist); and

8.3.2. information obtained in the course of carrying out the procedure (i.e. supporting documentation to verify the identification of the customer); and

8.3.3. such other information (if any) about the procedure as is specified in the AML and CTF Act.

8.4. Records in respect of financial transactions are to be retained for 6 years after the date of the transaction.

8.5. AML and CTF Program and addendums together with any documentation relevant to the reason for amendment are also to be retained for 6 years after the adoption of the AML and CTF Program and/ or amendments cease to be in force.

9. Financial Intelligence Unit (FIU) Feedback

9.1. FIU is the main AML and CTF regulator. FIU's role is to monitor PPB's compliance with the AML/CTF legislation.

9.2. FIU may provide PPB with feedback in respect of its performance on the management of ML/TF risk. FIU also has the power to compel licensees to produce certain information.

9.3. The receipt of any notice, direction or recommendation from FIU will be immediately referred to the AML and CTF Compliance Officer.

9.4. Notices from FIU may include the following:

9.4.1. to compel production of information or documents;

9.4.2. to enter premises under a monitoring warrant;

9.4.3. to require an external audit or AML and CTF risk assessment;

9.4.4. to provide remedial direction; and

9.4.5. to accept enforceable undertakings.

9.5. The General Counsel and Chief Compliance Officer as well as AML and CTF Compliance Officer (s), in conjunction with other Representatives, will take all steps necessary to comply with any feedback, notices, orders, warrants etc or to implement any directions issued by FIU.

9.6. The AML and CTF Compliance Officer will prepare appropriate reports for FIU. Reports required by law or by FIU will be forwarded within the period specified in such law or any notice or order or if FIU allows a longer period, that longer period.

9.7. The General Counsel and Chief Compliance Officer as well as AML and CTF Compliance Officer (s) will have due regard to any feedback provided by FIU in respect of PPB' performance in managing its ML/TF risks. Such feedback will be incorporated into ongoing monitoring programs and the AML and CTF Program will be amended (where appropriate).

9.8. The General Counsel and Chief Compliance Officer will be responsible for the implementation of any specific recommendations made by FIU to PPB in respect of its ML/TF risk management performance.

9.9. The AML and CTF Compliance Officer (s) will monitor FIU information sources, circulars, and guidance notes, in respect of domestic and international issues which may affect the business. This includes financial sanctions and updates to lists of terrorist groups.

10. Independent review of AML and CTF Program

10.1. A review of Part A of the AML and CTF Program will be undertaken annually by the General Counsel and Chief Compliance Officer together with the review of the whole Program and Policy or as part of conducting independent AML/CTF risk assessment.

10.2. The review of the Program and/or independent AML/CTF risk assessment may be also undertaken by an external service provider that will be retained to conduct the review (outsourced independent assessment as third line of defence).

10.3. The purposes of the review will be to:

10.3.1. assess the effectiveness of the AML and CTF Program, having specific regard to the ML/TF risks faced by PPB;

10.3.2. assess whether AML and CTF Program complies with the AML and CTF Act;

10.3.3. assess whether Part A of the AML and CTF Program has been effectively implemented; and

10.3.4. assess whether PPB have complied with the AML and CTF Program.

10.4. The result of the review, including any report prepared, will be provided to the Board of Directors.

11. Systems to re-assess risk

11.1. PPB will continue to review all areas of its business to identify potential ML/TF risks that may not be covered in the procedures described above. The additional areas of ML/TF risks are in respect of new products, services, distribution channels and developing technologies.

11.2. Additional procedures to address these ML/TF risks are as follows:

11.2.1. General Counsel and Chief Compliance Officer will be consulted by any person having responsibility for a new service or method of delivery or new technology ("the project manager") at design stage or prior to the introduction of the new service, delivery method or technology. He will be required to advise on the ML/TF risk factors which are to be considered having regard to:

11.2.1.1. the target market (customer type);
11.2.1.2. the service features;
11.2.1.3. foreign jurisdictional features / offerings;
11.2.1.4. any electronic access to / the delivery method of the service;
11.2.1.5. the business structure and process.

11.2.2. The General Counsel and Chief Compliance Officer or appointed responsible AML and CTF Compliance Officer will, in consultation with the project manager undertake the risk assessment and formulate the controls and systems to manage any ML/TF risks.

11.2.3. The General Counsel and Chief Compliance Officer or appointed responsible AML and CTF Compliance Officer will review the AML and CTF Program, policies and procedures to ensure that any new ML/TF risks are identified in the AML and CTF Program and amendments to the AML and CTF Program are made. All amendments will require Board approval.

11.2.4. The General Counsel and Chief Compliance Officer or appointed AML and CTF Compliance Officer will formulate staff awareness and training programs in respect of the change to ML/TF risks and will oversee the delivery of training programs.

11.2.5. All records relevant to the risk assessment, addendums to the AML and CTF Program and the training programs are to be retained.

11.2.6. The General Counsel and Chief Compliance Officer or appointed AML and CTF Compliance Officer will ensure that any government or FATF findings concerning the approach to money laundering and terrorism financing prevention in particular countries or jurisdictions, is assessed and appropriate amendments made to the AML and CTF Program. Furthermore, all compliance procedures will be made and communicated to all Representatives.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML AND CTF) PROGRAM
PART B

1. Introduction

Part B of the AML and CTF Program sets out the Customer identification and verification procedures (also referred to as "Know you Customer" or "KYC" procedures). The AML and CTF Act requires any Reporting Entity (such as PPB) to carry out procedures to verify a customer's identity and other required information **before** providing any service to that customer.

Furthermore, ongoing due diligence of customers must be conducted. Where a review of a customer, business line or other circumstance results in a **change in the risk profile** of an **existing** customer, then the customer identification procedures described in this Part B of the AML and CTF Program are required to be implemented according to the assessed risk.

Accordingly, the primary purpose of Part B of this AML and CTF Program is to set out the applicable customer identification and verification procedures for customers of PPB.

2. KYC Responsibilities

The client relationship managers (or other Representatives responsible for the client) have full responsibility for knowing their customers. Thus the KYC process, including the initial and ongoing due diligence measures, shall be carried out by the business person responsible for each client.

PPB's compliance unit has the responsibility to develop the KYC rules and ensure that they are up-to-date. Furthermore General Counsel and Chief Compliance Officer as well as AML and CTF Compliance Officers shall advise and supply the client relationship managers with information and regular training in relation to KYC matters, perform monitoring of KYC procedures including sample selected client reviews and engage in other AML and CTF risk management activities as defined herein.

The main components of the KYC process are:

1. Gathering Basic KYC information (including identity check),
2. Checking against sanction and other lists,
3. Assigning risk and due diligence level,
4. Applying enhanced due diligence measures,
5. Customer adoption process, and
6. Ongoing customer due diligence.

3. Gathering KYC information (including identity check)

The level of information which must be collected is risk based, i.e. dependent on the identified ML/TF risk posed to PPB having regards to the following factors:

(1) its customer types, including any Politically Exposed Persons

(2) the types of designated services provided;

(3) the methods by which the designated services are delivered;

(4) the foreign jurisdictions with which it deals.

There are different customer identification and verification procedures for different customer types. Customer types include:

1. individuals (natural persons);
2. legal persons (companies, incorporated associations, registered co-operatives, government bodies);
3. legal establishments (trusts, partnerships, unincorporated associations).

The client relationship manager shall, for each customer who seeks to become a client of PPB, gather a certain minimum level of KYC information, referred to as Basic KYC information and for the high risk customers perform enhanced due diligence which includes collecting additional information. Basic KYC information as well as additional information checklists for different types of customers are specified in Annex 1 (aligned with Schedule 2 Table A of the AML and CTF Regulation Order). Gathering of information also includes verification of the customer's identity. In addition, the general principles defined in this Program shall be applied.

If there are gaps in the Basic KYC information or if ambiguity or uncertainty occurs in relation to the information provided by a customer, additional questions shall be asked or additional documentation requested. Where the identity of the customer cannot be confirmed without doubt, or information on beneficial ownership and purpose and intended nature of the business relationship cannot be obtained, a business relationship **shall not be entered into**. In such cases, transactions initiated by the customer shall not be carried out.

Where the customer is introduced by a person acting as the customer's agent, customer identification procedures are to be undertaken in respect of both the agent and the underlying customer i.e. PPB considers both the investor and the agent as its customer.

PPB shall not keep anonymous accounts.

The identity check concerning a private individual or anyone representing a legal entity shall as a minimum include a review of identification documents such as a generally approved identity card or passport.

In the case of both private individuals and legal entities, risk-based measures shall be taken to establish the source of funds and beneficial ownership of assets involved. Beneficial ownership shall be established for all customers.

In the case of legal entities, trusts and similar arrangements, reasonable measures shall be taken to understand the ownership and control structure of the customer.

Reliable and independent documentation (original documents, certified copies) as well as other available reliable sources (public electronic data, data warehouses etc.) shall be used to verify customer identity and other information provided. For client identity verification only original documents or duly certified copies shall be appropriate, copies are acceptable only for additional supporting documents.

3.1.Non-face-to-face customers

PPB shall apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview.

In order to mitigate the higher risk which may arise due to non-face-to-face customer PPB shall apply additional risk reducing measures such as: require certification of documents presented or additional documents to complement those which are required for face-to-face customers, initiate independent contact with the customer, use third party introduction, seek verification of the source of funds for the initial deposit, including sighting documentary evidence confirming the source of the funds etc.

3.2.Correspondent banking

PPB shall gather sufficient information about their respondent banks to understand fully the nature of the respondent's business before starting the correspondent banking relationship.

The information required shall 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.

PPB shall 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 and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

PPB shall not enter into or continue a correspondent banking relationship with a Shell Bank. Furthermore, appropriate measures shall be taken to ensure that PPB does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a Shell Bank.

4. Checking against sanction lists etc.

Specific regulatory restrictions and sanctions regarding certain subjects and/or jurisdictions must be observed (e.g. EC regulations passed from time to time with respect to particular political or terrorist entities, OFAC sanctions etc.). In addition, based on a risk assessment and relevant legal prerequisites, new and existing customers shall be checked against relevant external and/or internal watch lists.

PPB strictly follows the sanctions imposed in the jurisdictions in which it operates and sanctions of international institutions and regulatory bodies. If there's a sanction applicable to the customer or party of the transaction, it will restrict PPB from doing business with those certain individuals, entities and countries.

All monetary transactions and related data (accounts, involved parties) are to be individually and manually screened against sanctions lists. PPB uses third party service provider Accelus for sanction screening solution, i.e. World Check database, which is updated every day twice a day and covers 400+ sanction, watch, regulatory and law enforcement lists (including, but not limited to: OFAC, EU, UN, UK HMT).

The sanction screening strictly applies to every incoming and outgoing payment and is performed manually by the Representative in PPB responsible for the transaction (client relationship manager and in certain cases AML and CTF compliance officer).

Where a positive result is returned in respect of a customer i.e. the name appears on the relevant list, the AML and CTF Compliance Officer must be notified immediately and is responsible for overseeing the ongoing treatment of the customer and where applicable, making all reports, liaising with enforcement offices and reporting to the Board.

Any requests for third party payments will require that the name of the third party to be identified, verified and checked. Where a positive result is returned in respect of a third party payee i.e. the name appears on the relevant list, the AML and CTF Compliance Officer must be notified immediately and is responsible for overseeing the ongoing

treatment of the customer and where applicable, making all reports, liaising with enforcement offices and reporting to the Board.

PPB relies on the information provided by the customer or information from other financial institutions unless it gives rise to suspicion that the information is unreliable or dishonest. Removing or falsifying any information that would identify that a customer or a transaction may be covered by a sanction is strictly prohibited.

Although based on the specifics of PPB's client base and volume of the transactions performed manual checks of every single transaction is an acceptable routine, additionally automated transactions screenings will be available with the launch of new core IT system of PPB[1]. The software will inter alia, include tailor-made AML software with the functionality of an AML alert system, integrated with renewable external World Check's database (for sanctions lists and other available information) and enhanced by internally developed criteria and scenarios (such as certain threshold amounts, search words and other automatic features) triggering automatic AML alerts to responsible people, automatic FIU report filing, payment freeze feature etc. The system will also allow for the creation of White Lists and will have other features created to augment the due diligence level and automate some of the manual operations of PPB. After the launch of the AML alert system, the process and procedures on the features will be described separately or this Part B of the Program shall be updated.

All customers and beneficial owners have to be screened against applicable sanctions during the client take-on and continually over the course of the relationship. Depending on the individual, entity or country involved, transactions/accounts/assets of sanctioned parties must be blocked.

In addition, if a legal entity customer is assigned enhanced due diligence, the directors, authorized signers and powers of attorney related to the customer have to be screened, initially, in conjunction with client take-on, and risk-based on an ongoing basis.

Any breach of sanctions regimes must be reported to the competent authorities in accordance with local laws or regulations. In such cases General Counsel and Chief Compliance Officer shall be notified. PPB shall keep a logbook of accounts whose funds have been frozen.

5. Assigning risk and due diligence level

[1] Available after launch of the new Core banking system with AML alert functionality. Expected to go live in September 2015

The **risk ranking** procedure for new customers is set out in Annex 2. This procedure must be utilised by Representatives to categorise (or rank) a new customer and assess that new customer's risk profile as being high, medium or low.

If the customer's profile is ranked as high risk, further enhanced due diligence procedures must be applied as described herein.

The following circumstances shall indicate the high risk and enhanced due diligence level accordingly:

5.1. A check against a sanction list or watch list reveals that the customer or persons associated with it potentially may be listed on one or more lists,
5.2. Circumstances indicate that the customer (or persons associated with it, in the case of a customer that is a legal entity) is a PEP,
5.3. The customers´ behaviour or other circumstances indicate high risk,
5.4. The customer, following the risk ranking procedure, is seen as representing high risk, e.g. due to customer-, country-, product and services- and/or combination risks;
5.5. Other risk variables as indicated in paragraph below trigger high risk.

6. Applying enhanced due diligence measures

Based on an assessment of ML/TF risk PPB has identified certain risk variables which **will** trigger the requirement for additional KYC information and verification procedures to be performed (these depend upon customer type and that customer's risk profile).

The risk variables are:

(1) Where the prospective customer (natural person, director, member of governing body, beneficiary or beneficial owner) is named in a government list or a credible source's list;

(2) Where the risk of terrorism is identified;

(3) Where the customer, who is an individual (natural person), is a PEP or is known to have a link to a PEP;

(4) Where a non natural person is a PEP or is known to have a link to a PEP (this includes any directors, beneficial owners, beneficiaries and agents as the case may be);

(5) foreign jurisdiction risk (individuals and non-natural persons) i.e. the place the customer is domiciled (located) is considered high risk. In the case of non-natural person this includes officers and beneficial owners and beneficiaries;

(6) In the case of a listed company, the foreign jurisdiction risk with respect to the location of the exchange on which the listed company is traded;

(7) The customer has sophisticated activities and/or has links with high risk foreign jurisdictions;

(8) the customer's business activities place it in a higher risk category;

(9) Where intermediaries exist that are not Reporting Entities;

(10) Where the prospective customer is not physically present for identification purposes;

(11) Complex customer structures with numerous layers e.g. trusts;

(12) The customer structure does not support the disclosed business of that customer e.g. in the case of partnerships;

(13) Products & services risk;

(14) Services are provided exclusively via the internet.

The Enhanced Customer Due Diligence must always be applied when:

1) The Bank determines under its risk-based systems and controls that the ML and TF risk is high; or
2) a suspicion has arisen for the purposes of sections 20, 21, 22, 23 or 24 of the AML&CTF Act (suspicious transaction, suspicious activity, transaction conducted by money laundering entities, transactions involving terrorist property, transaction with no legitimate purpose); or
3) a party to the transaction, which the Bank is entering into or proposing to enter into, is physically present in, or is a business incorporated in, a prescribed foreign country (country linked with terrorist organizations).

With regard to high risk customers and/or business transactions the following measures shall be applied by the Representatives:

1) regularly collect information from the customer or from third party sources in order to update Banks knowledge (derived from the enhanced identification process) of the customer (i.e. conduct regular reviews of the customer information);
2) undertake more detailed analysis of the customer information including examining as far as possible the background and purpose of the transaction and business relationship;
3) regularly verify or re-verify the customer information in accordance with the customer identification process;
4) undertake more detailed analysis and monitoring of the customer's transactions - both past and future, including, but not limited to:

(i) the purpose or nature of specific transactions; or
(ii) the expected nature and level of transaction behaviour;

5) seek senior management approval for:
(i) establishing or continuing with a business relationship with a customer; or
(ii) whether a transaction on an account should be processed; or
(iii) whether the service should commence to be provided or continue to be provided to the customer;

Furthermore for a customer ranked as high risk customer the measures deemed relevant of the following shall be applied (the measures listed under 1 and 2 below are obligatory every time):

1. Verification of the beneficial owners by reviewing supporting documents on beneficial ownership information provided by the client or third parties, such as shareholders ledger, and verification of the identity of the beneficial owners by requesting a copy of the beneficial owner's identity card or passport,
2. Screening the customer, beneficial owners and representatives of the customer against World Check's lists (sanction, PEP-lists and other watch lists),
3. Ask additional questions and request additional documentation, based on identified risks, ambiguities and uncertainties,
4. Take adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship,
5. Supplementary measures to verify the documents supplied, or require confirmatory certification by a credit- or financial institution,
6. Other appropriate measures (communication with several representatives of the client company etc.).

All enhanced measures applied shall be documented and the records kept. For the recording of CDD and EDD process of the new customer and for the existing customer review process the CDD Checklist provided in Annex 6 may be used as a reference.

If after enhanced customer due diligence has been conducted the Representative and/or the AML and CTF Compliance Officer determines that there remains a high risk of ML/TF, or that one of the grounds for reporting a suspicious matter to FIU has been met, the AML and CTF Compliance Officer, in consultation with senior management, will determine whether the circumstances are suspicious enough to warrant the account being placed in suspense or closed and whether it is a further suspicious matter and thus, reportable (see Annex 9 "Suspicious Matters Reporting").

PEP

Specifically if the potential customer is a PEP it falls into the high risk category and is subject to enhanced due diligence, enhanced verification and enhanced on-going due diligence procedures.

PPB shall investigate thoroughly the source of funds before accepting PEP as the client. Further measures shall be also taken in order to satisfy itself as to bona fides of the intended transactions of a PEP customer.

The handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk. Possible risk factors to consider are:

1. the level of (informal) influence that the individual could still exercise;
2. the seniority of the position that the individual held as a PEP;
3. whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

Provided that the above mentioned risk factors do not trigger any concerns for higher risks, the person shall not be considered a PEP, if he/she has lost his service with prominent public functions more than a year ago.

7. Customer adoption process

After having gathered and verified customer information and assigned risk and due diligence level, irrespective of the level of risk assigned the client relationship manager shall present his proposal to approve the client to the *ad hoc* **Customer Adoption Committee.** The Customer Adoption Committee consists of respective client relationship manager, Managing Director of PPB and General Counsel and Chief Compliance Officer, or other AML and CTF Compliance Officer dedicated by him. The customer shall only be accepted if all members of the committee support the acceptance.

In case of disagreement between Customer Adoption Committee members, the client can be adopted only if approved by the Board of Directors.

As regards the customer adoption process the following records shall be kept:

1. When and by whom was a decision taken on establishment of the customer relationship, and
2. If the customer was assigned high risk rank, the reason why, including the reasoning on which the Customer Adoption Committee approved it.

After relevant KYC procedures have been conducted by the responsible client relationship manager the decision to establish correspondent banking relationships with the financial institution falls within the competence of the Customer Adoption Committee.

8. Ongoing customer due diligence

The client relationship manager shall conduct ongoing due diligence of all business relationships to ensure that the KYC information is up-to-date. It shall be documented when a review was carried out and by whom.

The reviews of existing records shall also be performed when a transaction of significance takes place, when customer documentation standards change substantially, when there is a material change in the way that the account is operated or when client relationship manager becomes aware at any time that it lacks sufficient information about an existing customer.

Periodic reviews shall be conducted:

1. For low risk customers - at 36 month intervals,
2. For medium risk customers - at 24 month intervals,
3. For high risk customers - at 12 month intervals.

The issue of changing the assigned risk level for a certain customer to higher risk or vice versa shall be handled by the relevant Customer Adoption Committee.

Other procedures of ongoing customer due diligence include the following:

1. Customers' transactions will be monitored on an ongoing basis in order to identify any unusual or suspicious activity or transaction;
2. Representatives will review transactions, including trading and electronic fund transfers, in the context of other account activity to determine if a transaction is suspicious;
3. the AML and CTF Compliance Officer (s) will be responsible for monitoring adherence to this Program and the AML and CTF Act, and will report suspicious activities to the appropriate authorities; the AML and CTF Compliance Officer will ensure that a sufficient sample of activity will be selected to enable the identification of matters of concern;

4. exception reports will be utilised to identify possible ML/TF risks and include monitoring transaction size, location, type, number and nature of the activity;

5. employee guidelines, with examples of suspicious money laundering activity and lists of high-risk customers whose accounts may warrant further scrutiny, will be prepared; and

6. the AML and CTF Compliance Officer will conduct an appropriate investigation before reporting a suspicious matter.

In addition to regular reviews, circumstances may arise in which an otherwise low risk customer will be elevated to high risk.

For example, a customer on commencement of the relationship may be classified as low risk. However, after considering the customer's circumstances (such as financial resources) and as a result of a change in activities, the risk profile of the customer may be elevated to high.

In circumstances where the customer's risk profile is elevated, further measures and controls will be implemented to mitigate and manage against potential ML/TF risks, including the following:

1. Immediate notification to all appropriate representatives / business units;

2. further KYC information and verification procedures performed;

3. an increase in the level on monitoring (i.e. in accordance with the new classification or rating of the customer risk, being medium or high and monitoring intervals commensurate with the identified risk).

9. Employee Due Diligence procedures / checks

There is a requirement within the AML and CTF Act to perform due diligence on certain representatives of PPB i.e. staff, employees, contractors, those seconded to the company for an interim period etc. The level of due diligence required depends upon the function performed and level of seniority / work performed.

The employee due diligence program includes appropriate risk-based systems and controls for PPB to determine whether to, and in what manner to, screen any prospective employee and also re-screen an employee (where that employee is transferred or promoted) that may

be in a position to facilitate the commission of a money laundering or financing of terrorism offence in connection with the provision of a designated service by PPB.

The employee due diligence program also establishes and maintains a system for PPB to manage any employee who fails, without reasonable excuse, to comply with any system, control or procedure established in accordance with Part A or Part B of this AML and CTF Program.

PPB has prepared a Recruitment Policy which covers the vetting of candidates for employment, taking and checking of references and the procedures to be followed in the recruitment process (see below paragraph).

The Recruitment Policy requires the Managing Director to conduct a formal interview of the candidate. PPB may also perform skills assessment, reference checks or any combination of these prior to offering a candidate a position. Representatives will be selected on the basis of their experience, skills, qualifications and industry knowledge.

The status of all new members of staff must be identified on their commencement of employment (authority to represent the company and provide a designated service) and the identification must be verified and recorded i.e. PPB will ensure that the identity and past history of a prospective employee (representative) has been verified prior to employment or authority granted to represent the company.

Once employed (or appointed to represent the company), Representatives that are identified as "high risk" will be subject to closer and more frequent monitoring. This includes monitoring of the representative's customer accounts and relationships (i.e. monitoring will be undertaken more frequently than that prescribed by the regular intervals pursuant to internal review procedures). In addition, these representatives may be subject to transactional limits until such time that comprehensive training in policies and procedures has been completed.

Examples of representatives to be considered as "high risk" include the following:

1. Representatives who are in a position of dealing with customers or circumstances which are identified as high risk.
2. Representatives in "key" positions.
3. Representatives that provide unusual or extraordinary activities.

4. Representatives who fail to conform to the company's compliance systems and/or controls[2].
5. Staff promoted to more senior levels with greater AML and CTF responsibilities that are yet to complete further AML and CTF training in policies and procedures.
6. Representatives which qualify as "high risk" for other reasons such as for example leading of lavish lifestyles, which cannot be supported by the representative's salary or other practical reason.

The level of staff turnover will also be considered and monitored on a regular basis.

Employee accounts are subject to the same AML and CTF procedures as customer accounts, under the supervision of the AML and CTF Compliance Officer.

The performance of supervisors with respect to compliance with the AML and CTF Act obligations will be monitored as part of their annual performance review.

Representatives who fail to comply with the compliance systems and/or controls will be subject to disciplinary procedures, which may include termination of employment (cancellation to represent the company). Representatives that are suspected of facilitating money laundering or terrorism financing will be additionally reported to the appropriate authorities.

10. Intermediary and introduced business

In some instances, PPB may rely on the procedures undertaken by other banks or introducers when business is being referred.

Prior to establishing relationship with such intermediary or introducer (hereinafter – intermediary), PPB should satisfy itself that the intermediary:

1. is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record-keeping requirements;
2. is fit and proper and is exercising the necessary due diligence in accordance with the standards applicable to PPB;
3. comply with the minimum customer due diligence practices as applied by PPB;
4. has reliable systems in place to verify the identity of the customer;
5. allows PPB to verify the due diligence undertaken by the introducer at any stage.

[2] Representatives who fail to comply with the compliance systems and/or controls will be subject to disciplinary procedures, which may include termination of employment (cancellation to represent the company).

All relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to PPB, who must carefully review the documentation provided.

In addition PPB shall conduct periodic reviews to ensure that an introducer that it relies on continues to conform to the criteria set out above.

PPB shall not rely on introducers that are subject to weaker standards than those governing PPB's own KYC procedures or that are unwilling to share copies of due diligence documentation.

There must be a written agreement in place for the management of the customer identification records whereby *inter alia* PPB has the right to access the records made by the agent and has the right to request information on their compliance procedures applied as well as request copies of the records made by the agent.

11. Client accounts opened by professional intermediaries

When PPB 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.

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

Where the funds are co-mingled, PPB should look through to the beneficial owners. There can be circumstances where PPB 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 PPB. PPB shall 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, PPB shall apply the criteria set out for intermediaries and introduced business, in order to determine whether a professional intermediary can be relied upon.

Where the intermediary is not empowered to furnish the required information on beneficiaries to PPB, 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 AML AND CTF Act or anti-money laundering legislation in other jurisdictions, then PPB should not permit the intermediary to open an account.

12. Discrepancies

If a discrepancy exists between information collected and verifying documents, then the Representative will take steps to resolve the discrepancy (where possible) and will record the steps taken. Additional measures may include:

1. An explanation from the customer in respect of the discrepancy together with supporting documentation;
2. Copies of transaction records (e.g. recent bank statement within previous two months);
3. Copies of other transaction documents;
4. Copies of management body's decisions;
5. Extracts from public governmental registers or other relevant registration body's certification etc.

The action to be taken will depend upon the discrepancy and will vary according to customer type and that customer's risk profile.

13. Disclosure Certificates

Where information is to be verified and it is not otherwise reasonably available from independent verification sources, a Disclosure Certificate may be provided from the customer (other than where the customer is an individual). This will constitute a reliable and independent document. Under no circumstances can a Disclosure Certificate be relied upon in verifying the identity of a customer where that customer is an individual.

The Disclosure Certificates are accepted by PPB only for those customers that have been classified or ranked as low to medium risk.

A Disclosure Certificate will not be accepted as suitable evidence to verify information where factors exist which result in the elevation of the ML/TF risk and the customer receives a high risk classification (ranking).

In cases where a company/trust/partnership/co-operative/association is established in Vanuatu or in other comparable jurisdiction and is subject to regulatory oversight similar to that of Vanuatu in its country of origin and/or principal operations (both have to be comparable jurisdictions), a Disclosure Certificate may be acceptable where information relating to beneficial ownership or other information is not otherwise reasonably available

from other verification sources. The copy of the identity document of the beneficial owner shall be always collected as a minimum in addition to Disclosure Certificate.
Where the company is not subject to regulatory oversight similar to that of Vanuatu in its country of origin and/or principal operations (non-comparable jurisdiction), a Disclosure Certificate may not be relied upon.

The information provided in Account Opening Form and other related forms filled in and signed by authorised customer representatives are deemed to act as proper Disclosure Certificates. Disclosure Certificate may have any other form acceptable to the Bank.

In these circumstances where the identity cannot be readily verifiable to the reasonably satisfaction of the representative (or agent or intermediary), the matter will be referred to a senior manager, who in consultation with the AML and CTF Compliance Officer, will determine whether PPB will enter into a customer relationship.

14. Customer refusing to provide information

If a prospective customer either refuses to provide information when requested, or appears to have intentionally provided misleading information, PPB will not accept the prospective customer (i.e. open the account) and will not do business with that person until the information has been provided and the customer identification and verification procedures as contained in this Part B of the AML and CTF Program have been satisfactorily completed.

If an existing customer either refuses to provide information when requested or appears to have intentionally provided misleading information, then PPB, after considering the circumstances and ML/TF risks involved, will consider closing the account.

In either case, the AML and CTF Compliance Officer will be notified in order to determine whether the circumstances constitute a reportable matter and whether the risk classification of the customer should be increased.

15. Forgery

Representatives responsible for the collection and verification of KYC information are not required to necessarily investigate whether a document provided by a customer has been validly issued. For example, representatives (or agents or intermediaries) can rely on documents issued by a governmental or statutory body as reliable and independent documentation and thus, verification of a customer's identity.

If, however, the document exhibits signs of fraud (tampering with the document), then the matter must be immediately reported to the AML and CTF Compliance Officer and he will

consider the factors in determining whether PPB can form a reasonable belief as to the customer's true identity and whether there's a matter of reporting to official authorities.

16. Recording the collection and verification procedure

Representatives responsible for the collection and verification of customer identification will record the verification procedure, including all identifying information provided by a customer, details of the verification methods used and the results of the verification.

Furthermore, where a discrepancy arises (in the verification process) Representatives shall record the method and result of the resolution of any discrepancy in identifying and verifying information.

Any additional information or verification procedures are to be documented and copies of any supporting documents (evidence) provided by the customer or obtained electronically by Representatives are to be retained as part of the records.

The Account Opening Form containing most of the KYC information together with other related forms filled in and documents provided by the customer during the account opening procedure shall be kept as a record of customer information collection.

The client risk profile assessment shall be recorded using Customer risk ranking tool provided in Annex 2 and saving a pdf-printed copy of the results as well as other methods of customer risk assessment and documenting the conclusions of the assessor.

For the recording of CDD and EDD process of the new customer and for the existing customer review process the CDD Checklist provided in Annex 6 may be used as a reference.

All customer identification records and any records made in respect of the verification process must be retained **for six years** after the closure of the customer account.

17. Requests for additional information from customers

If PPB determines that a prospective (or existing) customer has information that is likely to assist it in assessing, mitigating and managing its ML/TF risk, then PPB will provide notice to the prospective (or existing) customer requesting that information from them in accordance with Vanuatu Law.

For example, a corporate customer may have a complex business structure for which the identification of the underlying beneficial owner is not readily identifiable. In this

situation, requests will be made to the customer requesting clarity as to the structure. The sample form for such requests is set in Annex 3.

18. Authorised service providers and official source electronic data

PPB considers that data obtained from recognised government sources (or those of an equivalent regulatory standing) is reliable and independent and thus, a suitable electronic data source to be used for verification purposes.

PPB has determined that it will also accept electronic data available from authorised service providers (commercial carriers) provided the following criteria are met:

(1) The carrier is authorised to store personal data;

(2) The carrier uses a range of information sources that can be called upon to link an applicant to both current and previous circumstances;

(3) The carrier accesses negative information sources, such as databases relating to identity fraud and deceased persons;

(4) The carrier accesses a wide range of alert data sources; and

(5) The process is transparent i.e. it is clear what checks were carried out, details of the results and the level of certainty as to the identity of the prospective customer.

The following commercial carriers have been approved by PPB (the list may be updated any time):

- World Check by Accelus

PPB also uses and trusts various acceptable credible sources, sample list of which is provided in Annex 4

19. Foreign Jurisdiction

Certain foreign jurisdictions pose higher ML/TF risks than others due to the activities being conducted in those regions.

PPB considers Basel AML Index, found at http://index.baselgovernance.org/index/ being a credible source for jurisdiction risk ranking as well as other sources.

Without taking into account other circumstances, PPB considers countries with a Basel AML Index above 7 being high risk jurisdictions, countries which rank between 7 and 5 –

medium risk jurisdictions and countries with index 5 and below – low risk jurisdictions. When evaluating country risk its index falls with the limit values, 0,1 deviation is allowed to the closest risk definition, i.e. if the country's index is 5,1 the country may still be considered low risk jurisdiction, and vice versa if a country's index is 6,9 the country should be considered high risk jurisdiction.

In addition to that, the AML and CTF Compliance Officer will ensure that any government or FATF findings concerning the approach to money laundering and terrorism financing prevention in particular countries or jurisdictions is assessed and appropriately communicated to all Representatives, depending on their level of responsibility. Reports on FATF mutual evaluations are obtained from www.fatf-gafi.org.
The list of high risk jurisdictions as time to time updated is provided in Annex 5.