Anti-Money Laundering & Countering the Financing of Terrorism Policy

2024

Version Control

Revision Date	Version	Amendments	Author	Approver
01/06/2020	1	First Issuance to align to the Minimum Compliance Standards	Kelly Lam/ Kenneth Goh	PIAS Risk Committee
01/10/2021	2	Section 9.3 “Identifying Relevant Transactions – AML/CFT”. • Added further examples that pose a higher risk of money laundering	Kelly Lam/ Frankie Tan	PIAS Risk Committee
01/09/2022	3	Annual Review of AML Policy	Kelly Lam/Tang Ming Yang/ Maisuri Abdul Karim	PIAS Risk Committee
25/05/2023	3.1	Section 6 “Enhanced Customer Due Diligence (“ECDD”)” • Added High Risk Nature of Business - Occupation / Industries Section 6.1 “High Risk Factors leading to Enhanced Due Diligence (EDD) • 6.1a - Added High Risk Nature of Business - Occupation / Industries • 6.1a – Added customer being the subject of any Suspicious Transaction Reporting (“STR”) by PIAS to the authorities • 6.1d - Added High Risk Nature of Business - Table Section 8.6 “Global List Screening” • Edited Global List Governance section. Section 5.7 “Quality Checks” • Added QC sample size	Kelly Lam/Tang Ming Yang/ Maisuri Abdul Karim	PIAS Risk Committee

10/11/2023	3.2	Section 1 “Overview” • Edited AMLCFT policy to be reviewed once every year instead of once every 2 years Section 4.2 “Identifying, Assessing and Understanding Financial Crime Risks” • Added external TF risk environment, TF risk exposure, potential financing of other existing or new terrorist groups and new and emerging international typologies in which TF can be financed Section 9.2 “Transaction Monitoring Scenarios – AML/CFT” • Added four new scenarios/considerations Section 11 ”Suspicious or Unusual Activity Reporting – External” • Added a point sharing additional information or useful insights with Law Enforcement Agencies through the filing of supplementary STRs.	Tang Ming Yang / Mei Na Chua	PIAS Risk Committee
28/02/2024	3.3	Section 6.1 “High Risk Factors leading to Enhanced Due Diligence (EDD) • 6.1d - Edited High Risk Nature of Business – Table to remove Non-Profit Organisation from the list	Tang Ming Yang / Maisuri Abdul Karim	PIAS Senior Management Team

TABLE OF CONTENTS

1 Overview

Introduction

Money Laundering ("ML") is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities. The term "Money Laundering" is also used in relation to the financing of terrorism (where funds may or may not originate from criminal means).

Countering the Financing of Terrorism ("CFT") involves investigating, analysing, deterring, and preventing sources of funding for activities intended to achieve political, religious, or ideological goals. By tracking down the source of the funds that support terrorist activities, law enforcement may be able to prevent some of those activities from occurring.

Examples of money laundering include:

- where an organized crime gang carry out a series of staged motor accidents ("crash for cash"), successfully defrauding an insurance company. The insurance payouts are the proceeds of crime, which gives rise to money laundering when the gang receive their funds;
- where a successful drug trafficker uses the proceeds of his drugs sales to invest in a pension. The pension funds are the proceeds of crime, and the pension provider is potentially involved in money laundering;
- where a tax evader buys a life policy with the profits of his tax scam. The premium is paid with the proceeds of crime, and the insurer is unknowingly involved in money laundering. When the policy pays out, the tax evader will have laundered his criminal funds.

Examples of terrorist financing ("TF"):

- where a terrorist organization needs to insure a boat to move terrorists from one place to another. The insurance premium is terrorist financing, as it allows the terrorist organization to operate;
- where a terrorist organization is involved in "crash for cash" scam. When the insurance company pay-out is used to fund the living and operation of the terrorist cell, this will amount to terrorist financing, as well as money laundering.

Professional Investment Advisory Services Pte Ltd ("PIAS") is committed to ensure compliance with Group Financial Crime Policy, and all applicable regulations that may be issued by the relevant authorities in Singapore. The applicable local regulations for Anti-Money Laundering & Countering the Financing of Terrorism Policy are set out in Financial Advisers Act 2001 ("FAA") and Financial Advisers Regulations 2002 ("FAR").

Local guidance for Money Laundering and Countering the Financing of Terrorism are governed by Financial Advisers Act 2001 - Notice 06 on Prevention of Money Laundering and Countering the Financing of Terrorism - Financial Advisers ("FAA-N06"), Corruption, Drug Trafficking & Other Serious Crimes (Confiscation of Benefits) Act 1992, Terrorism (Suppression of Financing) Act 2002 and its subsidiary legislation.

For further information regarding the following:

1. Group Financial Crime Policy
2. Top-Level Commitment
3. Risk Preference Statements
4. Employee Culture
5. Third Party Culture
6. External Communications

Please refer to Sections 1.2 - 1.7 of the Financial Crime Risk Management Policy (FCRMP) 2022.

When the local regulatory requirements or obligations are set at a higher level than Group Financial Crime Policy, local procedures will be put in place to comply with those higher-level obligations, which are approved by the Money Laundering Reporting Officer ("MLRO"). Upon approval by the MLRO, changes will be made to the respective policies based on the higher regulatory requirements.

This policy shall be kept up-to-date and reviewed at least once every year, or when a material event occurs, whichever is earlier.

2 Accountabilities

For further details regarding the appointment and responsibilities of the 'Designated Individual', MLRO and Nominated Officer(s), please refer to the Financial Crime Risk Management Policy 2022.

3 Financial Crime Operating Model

The 'Designated Individual' is responsible for defining and implementing PIAS' Financial Crime Operating Model. For PIAS, the 'Designated Individual' is the Head of Risk Management & Compliance.

The operating model will:

- incorporate the Group's three lines of defence operating model
- set PIAS Risk Committee structure
- define PIAS' organizational structure for financial crime, allocating adequate resources with the appropriate skills, knowledge and experience to support both the 1st line and 2nd line of defence financial crime related activities
- consider appropriate segregation of duties to reduce the opportunity for financial crime to be committed by employees
- implement the Group's financial crime policy
- incorporate the Group's financial crime target process and technology end state
- be documented and regularly reviewed for continued relevance

For more details on the Financial Crime Operating Model, please refer to the Financial Crime Management Policy 2022.

3.1 Financial Crime Risk Management Programme

Within PIAS, the 'Designated Individual' is required to ensure that an appropriate Financial Crime Risk Management Programme("FCRMP") is designed, documented and implemented.

The purpose of the FCRMP is to set out how PIAS' Financial Crime Operating Model delivers compliance with applicable legal, regulatory and internal PIAS requirements. This will cover all financial crime risks relevant to PIAS.

For more details on the FCRMP, please refer to PIAS' Financial Crime Management Policy 2022.

3.2 Operating Model and Financial Crime Risk Management Programme Review

PIAS reviews the Financial Crime Risk Management Programme on a regular basis (at least annually), to ensure they are fit for purpose and reflect any changes to PIAS' risk profile. Additional reviews will be initiated where there are significant changes to the business, such as a merger, acquisition, disposal, major new product line/customer proposition, business transfer/ re-organization, new geographical market, new or revised legislation and/or regulation etc. At a minimum, the review process will be documented at PIAS Risk Committee.

Where there are changes to PIAS' financial crime operating model being proposed, PIAS' Head of Risk Management & Compliance (or equivalent) will obtain agreement to the changes from the Group Head of Legal and Compliance before the changes are made. This is to ensure that the financial crime operating models for all markets remain within the overall Group Financial Crime Operating Model.

4 Risk Assessment

4.1 Enterprise-Wide Risk Assessment

Appropriate steps are to be taken in order to identify, assess and understand its financial crime risk (or minimally the ML/TF risks) at the enterprise-wide level. The enterprise-wide financial crime risk assessment will enable the Group and PIAS to better understand its overall vulnerability to financial crime and to forms the basis for the overall risk-based approach across the Group.

The results of the reviews will be documented and approved by PIAS senior management even if there are no significant changes to the enterprise-wide risk assessment.

The assessment will be kept up-to-date and re-performed at least once every two years, or when a material trigger event occurs. Such material trigger events include but are not limited to:

- the establishment or acquisition of a new subsidiary; or

- the acquisition of new customer segments or new delivery channels, or the launch of new products and services by a subsidiary.

In performing the ML/TF aspects of the risk assessment, the following should be considered:

(a) the ML/TF risk environment of the countries in which we operate (e.g. this information can be obtained from the Singapore's National Risk Assessment Report and in particular, the industry sectors and the crime types that present higher ML/TF risks);

(b) the inputs from the Suspicious Transactions Reporting Office ("STRO") i.e. whether there is a high incidence of cases where we are instructed to take action to freeze assets;

(c) the target customer segments and customer profiles such as those identified as politically exposed persons, those from higher risk industries or countries, the value of the transactions, etc;

(d) the nature of products and services, i.e. whether the products carry a cash value or not, national insurance scheme versus voluntary life insurance, etc; and

(e) the channels of distribution employed including whether they are subject to equivalent AML/CFT regimes.

4.2 Identifying, Assessing and Understanding Financial Crime Risks

PIAS must identify, assess and understand the respective financial crime risks in relation to:

- the customers;
- the countries or jurisdictions the customers are from or in;
- the countries or jurisdictions they have operations in;
- the products, services, transactions and delivery channels;
- the external Terrorist Financing (TF) risk environment, including geographies with heightened TF risks, emerging typologies and common payment methods used;
- the extent of PIAS TF risk exposure, including the size of PIAS business, nature and complexity of PIAS business model or transactions;
- the potential financing of other existing or new terrorist groups regionally and globally; and
- the new and emerging international typologies in which TF can be financed, including through ransomware, arts and antiquities and online crowdfunding mechanisms.

In carrying out the above assessment, the following appropriate steps are to be taken:

(a) the risk assessments must be properly documented based on guidance from Group Financial Crime;

(b) the assessment must consider all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of risk mitigation actions/measures to be applied;

(c) the risk assessments must be updated when there is a trigger event or at least once every 2 years; and

(d) the results approved by PIAS senior management and shared with the Board. Thereafter, the risk assessment information may be provided to the Authority upon request.

4.3 New Products, Practices and Technologies

PIAS is to identify and assess the financial crime risks that may arise in relation to:

(a) the development of new products and new business practices, including new delivery mechanisms; and

(b) the use of new or developing technologies for both new and pre-existing products.

PIAS to perform a risk assessment prior to the launch or use of such products, practices and technologies. Appropriate measures must be implemented to manage and mitigate the financial crime risks in accordance with the risk-based approach for risk management.

Where the new products, new business practices including new delivery mechanism and new or developing technologies favour anonymity, the Group Head of Legal & Compliance approval is required prior to launch.

5 Customer Due Diligence ("CDD")

'Customer' means a person (whether a natural person, legal person or legal arrangement) with whom PIAS establishes or intends to establish business relations and includes in the case where PIAS arranges a group life insurance policy, the owner of the master policy.

PIAS identifies, verifies and evaluates the circumstances of the customer to ensure that it knows who it is doing business with, and that the customer is within PIAS' risk appetite. PIAS does not open or maintain an anonymous account or an account in a fictitious name for any customers.

PIAS conducts initial CDD activities for customers (individuals, corporates or other body of persons), beneficial owners and any connected party of the customers before the business relationship starts. CDD takes place at the start of the relationship and throughout the relationship in order to:

- identify and manage the financial crime risks to which PIAS is exposed and to minimize the impact of these financial crime risks on our customers and shareholders

- comply with legal requirements and regulatory expectations to undertake risk -based customer due diligence for certain product types and to apply enhanced customer due diligence standards in specific circumstances (e.g. where required in relation to the prevention of money laundering)

When establishing business relationship with individual customers, the following personal information about the customers are obtained:

- full name;
- unique identification number (such as an identity card, passport or birth certificate number);
- residential address;
- date of birth; and
- nationality.

PIAS also conducts CDD when there is a suspicion of money laundering or terrorism financing, or if PIAS has doubts about the veracity or adequacy of any information previously obtained.

5.1 Risk-Based Application of CDD

CDD is conducted according to the level of risk posed by the customers. The level of CDD required will be dependent on the financial crime risks associated with the type of customer, their location, the product involved and the nature of their engagement with any of PIAS' associated persons.

'Knowing your customer' is a key component of effective measures to combat fraud, sanctions breaches, bribery and other financial crime.

- Simplified Customer Due Diligence (SCDD) may be performed if PIAS is satisfied that the risks of money laundering and terrorism financing are low; Customer Due Diligence (CDD) is applicable as the standard level of due diligence;

- Enhanced Customer Due Diligence (ECDD) is applicable in all defined higher risk circumstances, where information over and above CDD is required (For e.g. screening of high-risk customers or politically exposed persons).

Individual customer risk assessments ensure that the risks a customer relationship brings to PIAS are captured and ensure due diligence measures and ongoing monitoring are effective and proportionate.

5.2 Customer Due Diligence

Customer due diligence ("CDD") means:

- Identifying the customer and verifying the customer's identity (individuals, corporates, or other body or persons;
- Identifying any beneficial owner of the customer (where relevant) and verifying their identity;
- Identifying the beneficiary (where relevant) and verifying their identity
- Identifying key corporate personnel (where relevant) and verifying their identity on a risk-based approach; and
- Identifying connected party of the customer
- Identifying beneficial owner of a beneficiary
- Assessing and obtaining information on the purpose and intended nature of the relationship

Individuals – Identification

Whilst the level and extent of customer information collected may vary, PIAS at a minimum collects the following information:

- Full name
- Unique identification number (identity card, passport or birth certificate number)
- Residential address
- Date of Birth
- Nationality
- Purpose and intended nature of the relationship
- In addition, to assist with name screening and risk assessment, PIAS collects the following information whenever possible:
- Gender

Individuals - Verification

The information provided to identify the customer must be verified using reliable, reputable and independent source documents, data or information. Government issued documentation is commonly used as a reliable source to verify the identification information provided.

Where someone is acting on behalf of a customer or beneficiary (e.g. trustee(s) or others such as those exercising power of attorney), PIAS must:

- verify that the person is authorized to act on behalf of the customer by obtaining appropriate documentation, providing authorization to act on behalf of the customer
- verify that persons identify to the same standard as the customer as above, using independent and reliable sources

Corporate Bodies - Identification

For corporate bodies, the following is the minimum information that PIAS obtains to identify the customer, any Beneficial Owners and the key corporate personnel.

- full name of entity
- company number or registration number
- the address of its registered office and principle place of business
- the law to which the entity/corporate is subject and its constitution (except where the entity/corporate is listed on a regulated market)
- names of board of directors and other senior persons responsible for the operations ('key corporate personnel')
- details of all shareholders or other beneficial owners with a shareholding/ownership of more than 25% of the entity
- details of business activity and/or sector
- purpose and intended nature of the relationship

Corporate Bodies - Verification

For companies, PIAS verifies the following information in relation to the company concerned:

- full name
- registered number
- registered local business office address

- country of incorporation
- names of beneficial owners (see Section 5.4)

PIAS takes reasonable steps on a risk-based approach to verify:
- the law to which the corporate is subject
- its constitution (whether set out in its articles of association or other governing documents)
- names of key corporate personnel (see above – the directors and the senior persons responsible for the entities operations)

PIAS may verify the information set out above, from appropriate sources, such as:
- confirmation of the company's listing on a regulated market
- a search of the relevant company registry
- a copy of the company's Accounting & Corporate Regulatory Authority ("ACRA") report

PIAS need not inquire if there exists a beneficial owner in relation to a customer in the following situations:

- an entity listed on a stock exchange outside of Singapore that is subject to:
  (i) regulatory disclosure requirements; and
  (ii) requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means);
- a financial institution set out in Appendix 1 of MAS Notice FAA-N06
- a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or
- an investment vehicle where the managers are financial institutions:
  (i) set out in Appendix 1 of MAS Notice FAA-N06; or
  (ii) incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, unless PIAS has doubts about the veracity of the CDD information, or suspects that the customer, business relations with, or transaction for the customer, may be connected with money laundering or terrorism financing

5.3 Relevant Parties for CDD Beneficial Owner(s)

In respect of individuals, the customer is the beneficial owner, unless there are features of the relationship, or surrounding circumstances, that indicate otherwise.

In respect of corporate bodies, the beneficial owners are individuals that either:
- own or control more than 25% of the shares or voting rights of the company; or
- otherwise own or control the customer.

In respect of a trust or similar arrangement, the beneficial owners include:
- the settlor;
- the trustees;
- the beneficiaries; and

- any individual who controls the trust.

These individuals (beneficial owners) must be identified, and reasonable measures must be taken to verify their identities through the collection of relevant information (as per the 'individual' or 'entity/corporate' information requirements listed below).

Beneficial owners may own or control the customer, directly, or indirectly through one or more intervening entities. Corporate structures must be examined to determine whether there are any entities between the customer and ultimate beneficial owner. In those circumstances, where beneficial owners own or control the customer indirectly through intervening entities, those intervening entities must also be identified through the collection of relevant information and they must be treated as 'beneficial owners'.

If no individual owns or controls more than 25% of the shares or voting rights in the body, PIAS will determine who are the individual or individuals that exercise effective control over the company. This individual (or individuals) could be:

- a shareholder with less than 25% of the shares or voting rights (e.g. a majority shareholder with 20% holding)
- an existing director of the company or its parent,
- a member (or members) of the company's executive/senior management team

If, and only if, PIAS has exhausted all possible means of identifying the beneficial owner but have not succeeded in identifying the beneficial owner or are not satisfied that the individual identified is in fact the beneficial owner, then the senior person in the entity responsible for managing the entity/corporate must be treated as the beneficial owner. In cases of doubt, PIAS may consult with Group Financial Crime where required.

Key Corporate Personnel

In addition to identifying Beneficial Owners, PIAS must identify those individuals exercising control over the entity and its relationship with PIAS. The following are the roles considered to be Key Corporate Personnel for customer due diligence purposes:

- Members of the board of directors or equivalent (e.g. management committee)
- Senior persons responsible for the operations of the corporate body
- The individual(s) within the corporate who manage the business relationship with PIAS (e.g. authorized signatories and instruction givers)

These individuals must be identified, and reasonable measures must be taken to verify their identities through the collection of relevant information.

5.4 Ongoing Customer Due Diligence (CDD)

PIAS monitors, on an ongoing basis, its business relations with customers.

PIAS determines the appropriate level of ongoing CDD appropriate for its customers and products, ensuring that the approach taken aligns to its risk appetite.

On-going CDD activities are considered on a risk-based approach, with the extent, frequency and nature of due diligence reviews or refresh driven by the risk posed by the customer in order to:

- ensure the CDD information is kept up to date and reflects any changes to the customer's details
- ensure it continues to meet legal or regulatory requirements
- ensure that the customer and their activities remain within PIAS' risk appetite

On-going CDD is conducted annually, on a trigger-event basis, or on a combination of the two.

Periodic Reviews

Periodic reviews can be set at a regular frequency which is based on the risk classification of the customer and follows a risk-based approach. All customers identified as 'high-risk' are reviewed on an annual basis. Periodic reviews may be most appropriate for corporate clients as their beneficial ownership, corporate structure and key personnel are more likely to change over time than is the case for individual customers.

Trigger Reviews

Trigger reviews are reactive in nature and are conducted upon the occurrence of a specific event (for example, change in the customer details/profile, detection of unusual activity, claim/redemption, additional contribution, returned mail, etc.).

The nature of ongoing due diligence will be proportionate to the risk, taking into account the frequency of customer contact/interaction, the longevity of our products, the length of the customer relationship, etc. For example, a customer paying regular premiums over 20 years, from the same account, responding to documentation sent to their address, with a low value product and no unusual activity, is unlikely to require frequent intrusive CDD.

Where possible, CDD reviews are to be completed from existing business information and public source data. PIAS only considers obtaining additional information direct from the customer if no other means of re-confirming CDD information is possible.

PIAS considers also that although keeping customer information up-to-date is required under AML/CFT legislation, it is also often a requirement of data protection legislation in respect of personal data.

5.5 Simplified Customer Due Diligence (SCDD)

There are circumstances where the risk of money laundering or terrorist financing is deemed to be low and MAS Notice FAA-N06 allows for reduced or limited CDD measures. In such circumstances and provided there has been an adequate analysis of the risk involved, PIAS may apply simplified CDD (SCDD) measures.

Where PIAS applies SCDD measures, it may adjust the extent, timing or type of measures taken to comply with the standard CDD requirements. SCDD is not an exception to completing CDD.

Where PIAS wishes to make use of simplified customer due diligence, they must document the circumstances with the rationale for the decisions made on each individual case when SCDD is applied.

It is important to note that no one factor automatically entitles the application of simplified customer due diligence. Each case must be considered on a case-by-case basis and all of the circumstances must be assessed to determine the risk posed by the customer. Only in circumstances where it is identified that the customer poses a low degree of risk of money laundering and terrorist financing may simplified due diligence be considered.

Where one part of the Singlife Group is itself a customer of another part of the group, it is expected that SCDD will usually be applied, where permitted under local legislation and in absence of any high-risk factors.

5.6 Reliance Placed on Others for the Identification and Verification of Customers

Where local legislation permits, PIAS may be able to rely, for CDD purposes, on the identification and verification work completed by an intermediary introducing the customer.

Where PIAS is able to, and wishes to, place reliance on the identification and verification work completed by another party (for example the intermediary introducing the business), PIAS will satisfy itself that the party relied upon is monitored or supervised for anti-money laundering purposes, including CDD and record keeping requirements, to at least the same level as the business placing reliance.

PIAS also consider the matters shown below before agreeing to rely on the identification and verification information provided by another party:

- the local legal/regulatory requirements for reliance
- the relied upon party's public disciplinary record, to the extent that this is available
- the nature of the customer, the product/service sought, and the sums involved
- any adverse experience of the relied upon party's general efficiency in business dealings
- any other knowledge, whether obtained at the outset of the relationship or subsequently, regarding the standing of the party being relied upon

If PIAS is reliant on the identification and verification of a customer by another party, PIAS will:

- ensure the relied upon party makes available all information about the customer (and any beneficial owner) obtained when applying CDD measures
- require the relied upon party immediately on request to provide copies of any identification and verification data and any other relevant documentation on the identity of the customer, customer's beneficial owner, or any person acting on behalf of the customer
- require the relied upon party to retain copies of the data and documents used to complete CDD in accordance with PIAS' record retention requirements
- regularly review, on a risk-based approach, the reliability of the relied upon party's identification and verification process and procedures. For example, where a confirmation certificate is used asking for a sample of identity and verification documents

- revert to their own identification and verification procedures where deficiencies are identified in the relied upon party's procedures through a review or receipt of inadequate evidence
- consider whether to re-review existing customers introduced by the relied upon party where deficiencies have been identified in their procedures
- undertake any enhanced due diligence activities required where the customer has been classified as higher risk or otherwise subject to ECDD requirements

Reliance for standard customer due diligence may not be placed where:
- the person being relied upon has performed simplified due diligence procedures, and not standard customer due diligence; or
- the person being relied upon is itself relying upon someone else to have performed the CDD measures.

All situations where reliance is used must be clearly documented within the Financial Crime Risk Management Programme. Whilst reliance can be placed on third parties to conduct CDD activities, the ultimate responsibility for compliance with local laws and regulations cannot be outsourced and will remain with PIAS.

Wherever possible and permitted by relevant legislation, it is expected that one Singlife group business will rely upon another Singlife group business for completion of CDD, where such opportunities exist.

PIAS remains responsible for ongoing monitoring of their customers, and ensuring customer data remains up to date, particularly if the intermediary originally relied upon ceases to have a relationship with the underlying customer.

NOTE: 'Reliance' is different from a business applying CDD measures by means of an agent or an outsourcing service provider. 'Reliance' occurs where the relied upon party is already completing CDD for their own purposes, whereas an agent or outsourcer will be completing CDD for our purposes only.

5.7 CDD – Quality Checks

Quality Check (QC) reviews are carried out based on the 5% Group requirement for PEPs and Sanctions (including prohibited country alerts) closed alerts respectively on a monthly basis. PIAS conducts quality checks on completed CDD, including SCDD and ECDD. The nature and extent of the quality checks is determined by the MLRO (or equivalent) and is documented as part of the approved Financial Crime Risk Management Programme.

Quality checking must include in its scope:
- all areas for onboarding customers,
- all customer types (e.g. personal and corporate)
- all forms of due diligence (e.g. simplified, standard and enhanced)
- all relevant product types
- new customers subject to due diligence
- existing customers subject to due diligence review/refresh

Quality checking must:

- be conducted by someone other than the person who originally completed due diligence
- be completed objectively assessing against PIAS' current due diligence requirements
- include a sufficient sample size to be representative of the scale of the business and volume of CDD completed
- be conducted regularly (e.g. monthly or as part of the ongoing CDD process)
- be planned so as to include all onboarding/CDD areas, teams and locations over time
- provide a conclusion of 'pass' or 'fail' for each CDD case reviewed (where 'pass' means that the defined level of CDD has been correctly applied, completed and evidence of CDD is appropriately recorded)
- be used to trigger re-completion of CDD for cases that 'fail'
- be used to identify and address systemic or repeated errors in CDD completion

The results of quality checking of CDD forms part of the regular Management Information provided to PIAS Risk Committee and to Group Financial Crime.

5.8 Inadequate CDD Obtained – New Customers

New customers (including their beneficial owners where relevant) that cannot be adequately identified and verified in line with PIAS' documented CDD requirements will not be onboarded as PIAS has no risk appetite for entering into such relationships.

Processes must be documented to ensure that if satisfactory evidence of identity cannot be obtained prior to the business relationship commencing, or within a reasonable timescale, the business relationship must not proceed further.

Consideration must also be given to whether the failure to produce appropriate evidence of identity merits a Suspicious Transaction Report ("STR") being lodged. Where a STR is lodged, PIAS will not commence or continue business relations with the customer or undertake any transaction for any customer.

5.9 Inadequate CDD Obtained – Existing Customers

Each customer (including the beneficial owner) will be risk assessed, and PIAS' Head of Risk Management & Compliance (or equivalent) provides a recommendation on whether to exit or retain the customer relationship (including additional compulsory controls and any CDD remediation work required) to PIAS CEO.

Should PIAS wish to retain the customer relationship, the PIAS CEO must agree to risk accept the continuation of the customer relationship and document the reasons why the continuation of the customer has been risk accepted.

Nothing in this section authorizes retention of customers for whom the applicable regulatory standards of due diligence are not met.

5.10 Exiting Customers for Financial Crime Reasons

PIAS ensures that where it is established that a customer relationship is outside of appetite, it is appropriately managed through to exit. This extends to all customer relationships, regardless of whether it is subject to AML/CFT regulation for CDD purposes or not.

This will occur where PIAS has no appetite for maintaining relationships with customers for whom:

- the required level of CDD has not or cannot be completed
- PIAS is unable to provide the level of ongoing monitoring necessary to ensure that any suspicions of money laundering and/or terrorist financing are promptly reported

Where a decision is taken to exit a customer relationship outside of PIAS' risk appetite, an appropriate exit strategy must be developed for the timely termination of the business relationship.

PIAS' strategy will:

- be tailored to the individual business relationship involved
- take account of other relationships held by the customer with the Singlife Group. This includes other direct or indirect relationships in the same market and in other markets. Unless specifically and individually approved on a case-by-case basis by PIAS' Head of Risk Management & Compliance or equivalent, a customer 'out of appetite' for one part of Singlife Group, must be considered 'out of appetite' for other parts of Singlife Group
- consider any local market impacts i.e. reputational impacts
- consider any local legal/regulatory restrictions
- require notification to the PIAS' money laundering reporting officer (or equivalent) of all financial crime exits
- require all financial crime exits to be reported to and monitored by PIAS Risk Committee (or equivalent)
- include suitable procedures for preventing the exited customer being re-accepted as a customer (e.g. inclusion on an internal list)
- consider the need for a suspicious activity report, including any necessary regulatory approvals for return of funds, completion of a transaction, etc.

In some circumstances, due to legal, regulatory and/or contractual reasons, it may not be possible to unilaterally end a relationship before a contract end date. In such circumstances, PIAS will consider whether the 'exit' can occur:

- upon product renewal (where possible)
- on the basis of a 'void' contract (e.g. if the initial application was fraudulent and/or incorrect, or the client has breached contract terms (e.g. missed payment))
- on agreement with the customer
- on PIAS' unilateral demand with approval by the relevant regulator

If an exit is not immediately possible, then PIAS must ensure that:

- PIAS is not in breach of any legal/regulatory requirement by maintaining the relationship (e.g. it may be against the law to hold a relationship with some individuals/entities, such as those subject to certain sanctions provisions)
- the relationship is subject to Enhanced Customer Due Diligence, including enhanced ongoing monitoring
- the reason for maintaining the relationship is recorded
- approval for maintaining the relationship is obtained from PIAS' Head of Risk Management & Compliance (or equivalent)
- the customer is prevented from obtaining additional products or otherwise increasing their exposure with PIAS

A record of all customers identified for exit and those actually exited, including rationale, must be maintained to facilitate internal reporting and any external reporting requirements.

6 Enhanced Customer Due Diligence ("ECDD")

ECDD is required in any situation which by its nature can present a higher risk of money laundering or terrorist financing.

The following are examples of situations where ECDD will be carried out:

- in any case identified by a market under its risk assessment where there is a high risk of ML/TF
- in any business relationship or transaction with a person established in a high risk third country (Singlife's Jurisdiction Index – Very High and High Risk countries)
- in any business relationship or transaction with high-risk nature of business based on occupations / industries
- if an individual customer or potential customer has been identified as a PEP, or a family member or known close associate of a PEP
- in any case where the business is entering into a correspondent relationship with a credit institution or a financial institution
- in any case where:
  - a transaction is complex and unusually large; or there is an unusual pattern of transactions, and
  - the transaction or transactions have no apparent economic or legal purpose
- for any customer where the MAS or other relevant authorities in Singapore identifies as presenting a higher risk for ML/TF

6.1 High Risk Factors leading to Enhanced Due Diligence (EDD)

In determining the circumstances that introduce a high risk of ML/TF, PIAS as a minimum considers the following factors:

(a) customer risk factors, including whether—
  - the business relationship is conducted in unusual circumstances
  - the customer is resident in a geographical area of high risk
  - the customer is from high-risk nature of business based on occupations / industries

- the customer is a legal person or legal arrangement that is a vehicle for holding personal assets
- the customer is a company that has nominee shareholders or shares in bearer form
- the customer is a business that is cash intensive
- the corporate structure of the customer is unusual or excessively complex given the nature of the company's business
- the customer was the subject of any Suspicious Transaction Reporting ("STR") by PIAS to the authorities

(b) product, service, transaction or delivery channel risk factors, including whether—

- the product involves private banking
- the product or transaction is one which might favour anonymity (e.g. a bearer bond/policy)
- the situation involves non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures
- payments will be received from unknown or unassociated third parties
- new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre - existing products
- the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country

(c) geographical risk factors, including—

- countries rated as 'Very High Risk' or 'High Risk' in Singlife's Jurisdiction Index

(d) nature of business risk factors, including the following which are adopted from Singlife Group—

S/N	Nature of Business	Occupation
1	Dealers in Precious Metals or Stones	- Directors/Senior Management (Precious Metals or Stones) - Buyer/Purchaser (Precious Metals or Stones)
2	Oil/Petroleum Industry	- Directors/Senior Management (Oil or Petroleum)
3	Money Services Business (exclude Banks)	- Money Changer - Debt Collector - Non-Office - Debt Collector - Office Based - Pawnbroker - Credit Controller

		- Moneylenders - Remittance Agents
4	Casino or Other Types of Gaming Operators	- Casino/Gaming/Gambling Worker - Directors/Senior Management (Casino or Gaming Operators)
5	Virtual / Digital Currencies	- Dealers/Traders of Digital/Virtual Currencies - Directors/Senior Management (Virtual / Digital Currencies)

The presence of one or more of the above risk factors will not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation. In making our determination, PIAS considers the factors in the context of its own risk profile as determined in its assessment of risk (see section 4). For example, provision of a low risk product, to a low risk customer, in a low risk country via a non-face-to-face channel is unlikely to result in the relationship being high risk.

6.2 Enhanced CDD Measures

Where the information collected as part of the CDD process is insufficient in relation to the money laundering or terrorist financing risk, PIAS obtains additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship. Where PIAS has determined that EDD is required, the additional due diligence documentation and information obtained must be consistent with the risks identified.

Approval must be obtained from PIAS' CEO for all relationships with PEPs/RCAs and High Risk customers (HRC).

Obtaining information on the source of funds and source of wealth of the customer and enhanced ongoing monitoring are mandatory for PEPs, their RCAs and HRCs.

6.3 Source of Funds ("SoF")

SoF refers to the origin of the funds involved in the business relationship or occasional transaction relevant to the PIAS relationship. It refers to the activity that generated the funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.

Where it is identified that the source of funds relates to a third party, appropriate due diligence must be undertaken on the third party and the relationship between the third party and the customer is fully explained together with the rationale for the payment coming from a third party. Where it is identified that the source of funds is generated in and transferred from an overseas jurisdiction, the reason for this must be fully understood.

For higher risk customers subject to enhanced due diligence, the Risk & Regulatory team must approve all third party and overseas payments in, where possible before the transaction is completed.

Where PIAS determines that the risk of the business is increased further by a combination of increased customer, product and/or geographical risk associated with the transaction, PIAS will consider, as part of its ECDD, whether the information regarding source of funds needs to be independently evidenced - for example, the production of the bank statement for the account in question.

6.4 Source of Wealth ("SoW")

'Source of Wealth' describes identifying how a customer or beneficial owner acquired their total wealth.

The information obtained must give an indication as to the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

Although PIAS may not have specific information or details about all the client's assets, it may be possible to gather general information from publicly available information i.e. commercial databases or other open sources, external confirmations and information provided by the client.

Where PIAS determines that the risk of the business is increased further by a combination of increased customer, product and/or geographical risk associated with the transaction, PIAS will consider whether the source of wealth information needs to be independently evidenced.

It is likely that a customer's (or beneficial owner's) source of wealth is obtained from various sources and therefore the level of evidence required will be determined by the level of risk posed by the customer.

Politically Exposed Persons ("PEPs") and their Relatives and Close Associates ("RCAs") may be in a position to abuse their public office for private gain. PEP/RCA status must form part of the customer risk assessment process to drive the depth, nature and frequency of due diligence.

6.5 Definition of Politically Exposed Person ("PEP")

A Politically Exposed Person ("PEP") comprises of a domestic politically exposed person, foreign politically exposed person or international organization politically exposed person. It may also be an individual entrusted with a prominent public function, which includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executives of state-owned corporations, senior political party officials, members of the legislature and senior management of international organizations.

What constitutes a 'prominent public function' may vary according to the nature of the function, jurisdiction and societal elements. However, 'junior or mid ranking' officials are specifically excluded from the definition of a PEP. In cases of doubt whether a particular individual holds a

'prominent public function', PIAS will refer to the Risk & Regulatory team, who may seek additional guidance from Group Financial Crime.

6.6 Former PEPs

This refers to any individual that previously held a prominent public function (as identified above) at any time in the previous 12 months.

This means that:

- Existing customers who were PEPs must continue to be treated as a PEP for at least 12 months following the date on which that customer ceased to be entrusted with that public function
- New customers who previously held a prominent public function within the preceding 12 months must be treated as a PEP at onboarding and at least until 12 months after the date on which that customer ceased to be entrusted with that public function

In individual cases of the highest risk, or where local legislation/regulation sets a different period, a person may be treated as a PEP for a period longer than 12 months from when they ceased to be a PEP. The decision to treat an individual as a PEP for a longer period must be documented and made by PIAS' Head of Risk Management & Compliance.

6.7 Relatives and Close Associates ("RCAs")

PIAS will also identify and appropriately manage relationships with any individual that is either a relative or a close associate ("RCA") of a current PEP.

PIAS' definition of an RCA as follows:

Relative/Family Member

- spouse, or civil partner of a PEP
- children, step children or adopted children of a PEP and their spouses or civil partner
- parents or step parents of a PEP
- siblings, step-siblings or adopted siblings of a PEP

Close Associate

- a natural person who is closely connected to a politically exposed person, either socially or professionally
- an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a PEP
- an individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP

The requirement to identify and appropriately manage RCAs only applies to RCAs of current PEPs (i.e. those still active in a PEP role). An RCA of a former PEP must not be subjected to enhanced due diligence measures solely because of their relationship to a former PEP and

enhanced due diligence will only be applied (or continue to be applied) if it is justified by PIAS' assessment of other risks posed by that individual.

PIAS classifies all PEPs and RCAs as High Risk Customers, and prior to forming any business relationships with them, approval is sought from PIAS CEO. Thereafter, the PEPs and RCAs are monitored continually based on PIAS High-Risk Customer List.

6.8 PEP Screening Activities

PIAS screens customer and non-customer relationships for PEPs and RCAs in order to identify and manage any that may pose a higher risk of money laundering.

Who must be screened?
Customers (including identified key corporate personnel and beneficial owners and beneficiaries of long-term insurance contracts), counterparties, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture partners) must be screened to identify PEPs and their RCAs.

What must be screened?
The full legal name (and any known alias) of the individual must be screened. Where available, other supporting data, such as date of birth, nationality, residence, occupation, etc. must be included as per the data requirements articulated in the GNS Global Standard Configuration document.

When must screening take place?
Screening must be conducted at the initiation of the relationship and at regular intervals in the course of the ongoing relationship. This includes when due diligence information is amended or refreshed and periodically to take account of updates to screening lists.

The beneficiary of a life insurance policy (and any beneficial owners of that beneficiary) must be screened once identified, and in all cases before any benefit is assigned or payment made.

The tolerance for the timing and frequency of screening aligned to PIAS' Risk Preferences is as follows:

"All screen-able party records (customers, connected parties, employees, etc.) will be screened within 2 business days of the record becoming in scope and available for screening and, as a minimum, every 2 business days up until the point that the party record is no longer in scope."

AND

"All PEP (and RCA) alerts will be investigated and a true/false decision reached within 10 business days".

Why is screening conducted?

Identification of a PEP or RCA (as defined above) must result in an assessment of the financial crime risk of that relationship and a documented decision of whether to commence, retain, reject or end the relationship.

These customers (including identified key corporate personnel and beneficial owners and beneficiaries of long-term insurance contracts) must be subject to enhanced customer due diligence (ECDD).

The results of PEP screening must be included within the due diligence records.

How must screening be completed?

PEP screening by PIAS must be completed using the GNS tool and configuration, unless an alternative tool has been assessed by PIAS, approved by PIAS Risk Committee and notified to Group Financial Crime.

Where screening is conducted by outside parties (e.g. outsourcers) the Risk & Regulatory team must approve any alternative screening. PIAS will remain responsible for ensuring that higher-risk customers, including PEPs are appropriately identified and managed.

Where PEPs screening (or elements of PEPs screening) is prohibited by local legislation, Risk & Regulatory team must document this, seek risk-acceptance from PIAS Risk Committee and Group Financial Crime.

More details on the operation of PEPs screening, including how to request variations from the standard configuration (e.g. adding a PEPs category), can be found in the Global Name Screening (GNS) document.

6.9 Treatment of Identified PEPs and RCAs

Associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture partners) that are identified as PEPs or their RCAs, must be subject to a risk - assessment to help determine the appropriate level of due diligence necessary.

In addition to the above, customers (including their identified key corporate personnel and beneficial owners and beneficiaries of long-term insurance contracts) identified as PEPs or their RCAs, must:

- be subject to an assessment of the additional risk introduced by the PEPs or RCAs
- be subject to enhanced due diligence
- have the customer relationship with PIAS approved by appropriate senior management
- be included on a suitable local register of PEPs/RCAs exposure
- be subject to ongoing monitoring

6.10 Timing of Risk Assessment

PEP/RCA relationships are risk assessed as soon as the PEP/RCA relationship is identified. This may be at the initiation of a relationship with PIAS, or in the course of a relationship in the case of customers that become PEPs/RCAs after initiating a relationship with PIAS.

PIAS conducts ongoing risk assessment of PEP/RCA to ensure that:

- individuals are treated as a PEP/RCA only for as long as is required, considering the risk, this policy and any local guidance
- changing circumstances relating to the PEP/RCA are considered (e.g. a PEP with a low influence role, may have been promoted over time to a high influence position)
- any internal considerations, such as change of appetite, the submission of a Suspicious Transaction Report (STR), or unusual activity in relation to the PEP/RCA are considered

6.11 PEP/RCA Enhanced Customer Due Diligence ("ECDD")

PIAS has implemented appropriate procedures, systems and controls to conduct ECDD on customers identified as PEPs or RCAs. ECDD must include:

- completion of relevant required Customer Due Diligence measures
- obtaining approval from senior management for establishing or continuing the business relationship with that person
- taking adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or transactions with that person
- conducting enhanced ongoing monitoring of that business relationship

6.12 PEP/RCA Screening – Quality Checking

PIAS operates a process of quality checking of PEP screening decisions. The nature and extent of quality checking is determined by the MLRO (or equivalent).

Quality checking must include in its scope:

- all types of PEP/RCA screening (e.g. customer and non-customer)
- all methods of PEP/RCA screening used (e.g. automated, manual, batch, real time and different tools used)
- new customers subject to PEP/RCA screening
- existing customers subject to PEP/RCA screening

Quality checking must:

- be conducted by someone other than the person who originally made the PEP/RCA screening decision
- be completed objectively assessing against PIAS' current PEP/RCA definitions as informed by this policy and any additional guidance issued by Group Financial Crime
- include a sufficient sample size to be representative of the scale of the business and volume of PEP/RCA alerts identified
- be conducted regularly (e.g. monthly or as part of the ongoing CDD process)
- be planned so as to include all screening areas, teams and locations over time
- true match escalation procedures have been followed
- provide a conclusion of 'pass' or 'fail' for whether the correct decision has been made

- provide a conclusion of ‘pass’ or ‘fail’ for whether there is adequate rationale and evidence to support the decision
- be used to trigger remediation for cases that ‘fail’ (in either category)
- be used to identify and address systemic or repeated errors in PEP/RCA decisioning

The results of quality checking of PEP decisioning forms part of the regular Management Information provided to PIAS Risk Committee and to Group Financial Crime. Quality checking is normally performed by Risk & Regulatory Team.

6.13 Recording PEPs/RCAs – PEP Register

PIAS maintains a register of PEP and RCA customer relationships. The register is kept up to date and is available to the MLRO (or equivalent) on demand.

The Register must also be available on demand to Group Financial Crime. Where necessary, as a result of data sharing restrictions, customer personal data may be anonymized for the purposes of providing the data.

6.14 Beneficial Owner who are PEPs/RCAs of a Customer

PIAS will establish and maintain appropriate procedures, systems and controls to identify if the beneficial owner of a customer is a PEPs or RCAs. This requirement applies to those beneficial owners identified under the business’s risk-based approach to customer due diligence and does not extend to any beneficial owners not subject to identification requirements.

Where a beneficial owner of a customer is identified as a PEPs/RCAs, PIAS must assess the level of risk that the involvement of the PEPs/RCAs brings to the customer relationship to determine whether the customer is higher risk and must be subject to ECDD. This assessment must consider:

- the extent of control the PEPs/RCAs has over the customer
- the nature of the customer’s business
- the underlying risk of the customer
- the underlying risk of the product
- the nature of the association of the PEPs/RCAs to other beneficial owners
- the source of funds relevant to the customer relationship with PIAS
- the extent to which the PEPs/RCAs is using their own funds
- any local regulatory guidance

The presence of a PEP/RCA as a beneficial owner of a customer does not automatically make that customer higher risk. Each relationship must be assessed on a case-by-case basis.

The presence of a PEP as a beneficial owner of a customer does not automatically mean that other beneficial owners/shareholders of the customer must be treated as a RCAs to that PEP.

Where it is established that the customer needs to be subject to ECDD because the PEPs/RCAs has significant control or the ability to use their own funds in relation to the entity, the PEPs risk

assessment, approval and register requirements outlined above must be followed in relation to the customer.

The provisions of this section also apply to where an individual equivalent or similar to a beneficial owner of a customer is identified as a PEP/RCA (for example, identified key corporate personnel).

6.15 PEPs/RCAs in Long-Term Insurance Products

Businesses that provide a customer with a contract of long-term insurance must establish and maintain appropriate procedures, systems and controls to identify if the beneficiaries of the insurance policy, or the beneficial owner of a beneficiary of such an insurance policy, are a PEP or RCA.

Where it is established that the beneficiary is a PEP/RCA (or is owned/ controlled by a PEP/RCA) the PEP risk assessment, approval and register requirements outlined above must be followed in relation to the beneficiary.

These requirements must be met before any payment is made under the insurance policy.

7 Associated Persons and Non-Customer Due Diligence

PIAS identifies associated persons and third-parties, in order to carry out appropriate and proportionate due diligence on them, in relation to their role in preventing financial crime including money laundering and terrorist financing. An associated person includes any person, corporate or individual that performs services for or on behalf of PIAS, which includes employees. The term encompasses a wide range of persons connected to PIAS who might be capable of committing money laundering on its behalf.

For further details on associated persons and non-customer due diligence, please refer to the Financial Crime Management Policy 2022.

8 Additional Screening

Exposure to financial crime risks may come from the location of PIAS' operations; the customer; associated persons; counterparties; investment; insured activity; etc. Identification of exposure to higher risk jurisdictions must form part of the risk assessment process - for example, for customer and associated person due diligence, country risk will inform the depth, nature and frequency of due diligence.

Group's Jurisdiction Index provides a blended assessment of country risk across multiple financial crime risk types. A more granular assessment of individual financial crime risks can be obtained from an extract of Group's Jurisdiction Index – available from the Group Financial Crime Team. Historical financial crime related information about an individual or firm can inform the decision-making processes of whether or not to enter into a relationship with that individual or firm and

whether additional due diligence activities and/or future monitoring is required. Screening customer, supplier, director, employee, beneficial owners, beneficiary and third-party data against global 'special interest persons/entities' (where there is an implication of specific criminal activity) watchlist is an efficient and effective method of obtaining such information. More details of the 'special interest persons/entities' watchlists is included within the Global Name Screening (GNS) Definition Requirements' document.

8.1 Jurisdiction Index – Creation and Maintenance

Group's Jurisdiction Index is maintained by the Group Financial Crime Team. The methodology and framework for the creation and maintenance of the index is reviewed regularly and approved by Group Financial Crime. The Jurisdiction Index analyses the level of financial crime risk associated to a particular country by assessing various political, economic and criminal factors to produce an objective, transparent country risk rating.

Each country in the JI is rated according to the overall level of financial crime risk. There are four possible ratings:

- Low risk
- Medium risk
- High risk
- Very High Risk

8.2 Jurisdiction Index – Market Restrictions

PIAS identifies and records exposure to Very High Risk and High Risk rated countries where it conducts business in, involving, with, or on behalf of, customers and counterparties based in, or customers or counterparties from, Very High Risk and/or High Risk rated special risk countries.

Potential or actual exposure to Very High Risk and/or High Risk countries must be appropriately risk- assessed and approved as follows:

Very High Risk Countries

- for all very high-risk country proposals, PIAS CEO approval is required in addition to Head of Risk Management & Compliance's (or equivalent) endorsement - it is noted that a delegated authority may be required in some segments to manage the volume and frequency of requests
- all very high risk country proposals to be recorded locally and included in an appropriate compliance or financial crime report to PIAS Risk Committee
- all very high risk country approvals are to be notified to Group Financial Crime in monthly management information reports which will be collated across the markets and included in relevant Group level reporting
- PIAS to notify Group Financial Crime prior to onboarding of certain Very High Risk country proposals (refer to Jurisdiction Index list) where an assessment can be conducted at Group Financial Crime prior to seeking approval from PIAS CEO in order to onboard the customer.

High Risk Countries

- for all high risk country proposals, approval from a suitably 'Designated Individual' is required (i.e. designated by PIAS' Head of Risk Management & Compliance/'Designated Individual' or equivalent)
- all high risk country proposals (approved or not) are to be recorded locally and included in an appropriate compliance or financial crime report to PIAS Risk Committee
- all high risk country approvals are to be notified to the Group Financial Crime Team in monthly management information reports which will be collated across the markets and included in relevant Group level reporting

Medium Risk and Low Risk Countries

- for all medium and low risk country proposals, they are deemed to have medium to low financial crime risk and PIAS may conduct business with these customers, and they will be subjected to CDD measures.

8.3 Jurisdiction Index – Market Deployment

PIAS documents how it will use Group's Jurisdiction Index country risk rating to help manage financial crime risk, meet the requirements for Very High Risk/High Risk countries (see above) and any local regulatory requirements relating to country risk.

PIAS Usage of the Jurisdiction Index

PIAS uses the Group Jurisdiction Index and the results of screening against the Index to help inform the nature, extent and frequency of:

- customer due diligence (note – in some markets, legislation may require enhanced due diligence in respect of customers, counter parties or business with certain higher-risk countries)
- transaction monitoring (note – in some markets, legislation may require enhanced due diligence in respect of transactions with certain higher-risk countries)
- associated person (non-customer) due diligence
- compliance monitoring
- training and awareness

8.4 Special Interest Person/Entity (SIPs and SIEs) Screening

PIAS maintains procedures, systems and controls to screen relevant in scope customer and non-customer relationships in order to identify and appropriately manage those with documented implication of involvement in financial crime.

These procedures, systems and controls must include provision for:

- ensuring all relevant in scope name data is provided for screening
- ensuring that all relevant data attributes required are provided for screening
- the effective management, investigation and oversight of alerts produced through screening

Who must be screened?

Customers (including identified key corporate personnel and beneficial owners), counterparties including suppliers, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture partners) must be screened to identify association to financial crime.

What must be screened?

The full legal name (and any known alias/trading or brand name) of the individual or entity must be screened. Where available, other supporting data, such as date of birth, nationality, residence, occupation, etc. must be included as per the data requirements articulated in the GNS Global Standard Configuration document.

When must screening take place?

Screening must be conducted at the initiation of the relationship and at regular intervals in the course of the ongoing relationship.

It is expected that the timing and frequency of screening will align to that used for PEPs and sanctions screening:

“All screen-able party records (customers, connected parties, employees, etc.) will be screened within 2 business days of the record becoming in scope and available for screening and, as a minimum, every 2 business days up until the point that the party record is no longer in scope.”

If the timing and frequency of screening differs (from PEP and sanctions screening) this must be documented and agreed by PIAS Risk Committee.

All relevant alerts must be investigated in a timely manner and a true/false decision reached within 30 business days from alert creation.

Why is screening conducted?

Identification of association to financial crime must result in an assessment of the financial crime risk of that relationship and a documented decision of whether to commence, retain, reject or end the relationship.

The results of screening must be included within the enhanced due diligence records where a customer has been identified as:

- a PEP or a relative and close associate of a PEP
- resident in or operating out of a very high risk or high risk country
- ‘high risk’ for any other reason

How must screening be completed?

Screening for association to financial crime by PIAS must be completed using the Group's GNS tool using the Group prescribed configuration unless an alternative tool and/or configuration has been assessed by PIAS, approved by PIAS Risk Committee and notified to Group Financial Crime.

Where screening is conducted by outside parties (e.g. outsourcers) the Risk & Regulatory team must approve any alternative screening. PIAS will remain accountable for ensuring that higher-risk customers are appropriately identified.

Where screening for association to financial crime for some or all of the expected populations is prohibited by local legislation, the Risk & Regulatory team must document this, seek risk-acceptance from PIAS Risk Committee and notify Group Financial Crime. More details on SIP/SIE screening can be found in the GNS Global Standard Configuration document.

8.5 State-Owned Companies ("SOC") Screening

Being able to identify a connection or relationship with a SOC, or a SOC executive, will help inform the financial crime risk assessment for existing and potential new relationships. In particular, it will assist in identifying bribery and corruption risk and PEP (AML) risk exposure.

An entity is considered 'state-owned' where the government or state (or their representative bodies) own or control 50% or more of the entity. However, entities with lower levels of state ownership may still introduce risk to PIAS, for example where public officials represent the entity or otherwise interact with PIAS (bribery risk); where the state concerned is subject to sanctions; or where the state concerned is otherwise considered high-risk.

Who must be screened?

SOC screening is a requirement for:

- all customer relationships (including identified key corporate personnel and beneficial owners) subject to enhanced due diligence
- all non-employee associated persons (non-customer relationships acting for or on behalf of PIAS) including their identified key corporate personnel and beneficial owners
- the target or counterparty of any corporate acquisition or disposal (including Joint Venture partners).

SOC screening may be deployed in other circumstances (e.g. to help inform standard customer due diligence) dependent upon the nature of the business relationship.

What must be screened?

The full legal name (and any known alias/trading or brand name/former name) of the individual or entity must be screened.

Where available, other supporting data, such as address, company registration number, etc. must be included as per the data requirements articulated in the GNS Global Standard Configuration document.

When must screening take place?

Screening must be conducted at the initiation of the relationship and at regular intervals in the course of the ongoing relationship.

It is expected that the timing and frequency of screening will align to that used for PEPs and sanctions screening:
"All screen-able party records (customers, connected parties, employees, etc.) will be screened within 2 business days of the record becoming in scope and available for screening and, as a minimum, every 2 business days up until the point that the party record is no longer in scope."

If the timing and frequency of screening differs (from PEP and sanctions screening) this must be documented and agreed by PIAS Risk Committee.

All SOC alerts must be investigated in a timely manner and a true/false decision reached within 30 business days from alert creation.

Why is screening conducted?

Identification of a connection to a SOC will contribute to an assessment of the financial crime risk of that relationship and a documented decision of whether to commence, retain, reject or end the relationship.

The results of SOC screening must be included within the relevant enhanced due diligence records.

How must screening be completed?

SOC screening must be completed using the Group's GNS tool using the Group prescribed configuration unless an alternative tool and/or configuration has been assessed by PIAS, approved by PIAS Risk Committee and notified to Group Financial Crime. Alternative or additional methods (e.g. one-time internet research or bespoke due diligence reports) may also be used subject to approval by the Risk & Regulatory team.

Where screening is conducted by outside parties (e.g. outsourcers), the Risk & Regulatory team must approve any alternative screening. PIAS remains accountable for ensuring that higher-risk customers are appropriately identified.

More details on SOC screening can be found in the Global Name Screening (GNS) Global Standard Configuration document).

8.6 Global List Screening

Official List Management

Group Financial Crime determines the government, regulatory and other externally produced lists

(collectively ‘official lists’) to be used for screening by PIAS. These are documented in the GNS Global Standard Configuration document.

Group Financial Crime ensures that the latest versions of the required official lists are implemented by PIAS (to accommodate additions/deletions by the list provider) within the agreed timescales.

Global Prohibited List

Group Financial Crime maintains the global prohibited list which will contain individuals and entities that PIAS does not want to enter into any form of business relationship with.

Global Auto-Closure List

Group Financial Crime maintains the global auto-closure list (sometimes referred to as a ‘whitelist’ or ‘good guys list’) of names that may create irrelevant matches to specific, reviewed, match list entries, where approval has been given to auto-close alerts arising from those names. This list will contain individuals and entities with whom PIAS is happy to enter into (or maintain) a business relationship even where screening could result in an alert being created.

Global List Governance

Group Financial Crime is responsible for agreeing the criteria for the addition of new entries to, and the deletion of existing entries from, the global prohibited list and the global auto-closure list and is responsible for determining any additions to or deletions from the global prohibited list and the global auto-closure list.

The GNS Business Support Team is responsible for the maintenance of both the global prohibited list and the global auto-closure list within the group’s screening system (GNS), adding new entries and deleting entries.

The GNS Business Support Team will load the global prohibited list and the global auto -closure list into GNS. Potential matches will be created against:

- the global auto-closure list - which will all be auto closed
- the global prohibited list - which will generate alerts for investigation

On the identification of a positive match against the global prohibited list, PIAS must not enter into the proposed business relationship or must seek to exit the relationship where it already exists. Where it is not possible to exit the relationship, the relationship must be managed accordingly, including being risk accepted by PIAS’ Head of Risk Management & Compliance (or equivalent) and reported to PIAS Risk Committee.

8.7 Screening using Internal Lists

This section applies to all local non-official lists of names used for screening purposes, collectively referred to as ‘internal lists’. If PIAS use (or proposes to use) additional lists containing non-public,

internal or other intelligence data, it will obtain approval from Group Financial Crime for the use of such data.

Local Prohibited Lists

Local prohibited lists include names collated to identify specific individuals or entities by name, with the intention to take some additional action in respect of identified matches. They may be known locally as ‘grey lists’, ‘black lists’ or ‘intelligence lists’ and may typically include details of known or suspected fraudsters, previously exited customers, etc. These lists are those that are not commercially or publicly available and are created by, for or on behalf of PIAS.

Local Auto-Closure Lists

PIAS may maintain local auto-closure lists (sometimes referred to as a ‘whitelist’ or ‘good guys list’) of names that may create irrelevant matches to specific, reviewed, match list entries, where approval has been given to auto-close alerts arising from those names. This list will contain individuals and entities with whom PIAS is happy to enter into (or maintain) a business relationship even where screening could result in an alert being created.

Local List Governance

In any case of doubt of whether a list falls within either category, advice must be sought from Group Financial Crime. Any proposal to use an internal list in a single market must be supported by PIAS’ Head of Risk Management & Compliance (or equivalent) and the PIAS Risk Committee for approval.

Any proposal to use an internal list in more than one market must be supported by PIAS’ Head of Risk Management & Compliance (or equivalent) and PIAS Risk Committee proposing the list, before seeking approval from Group Financial Crime.

The GNS system must not be used for screening internal local lists without approval from Group Financial Crime. Only the Group Financial Crime or GNS Business Support team will implement any requests to use GNS for screening internal local lists. The above requirements also apply to internal local lists currently in use. Any existing lists in operation must be reviewed and the process above followed if it is intended to keep using existing lists on an ongoing basis.

8.8 Other GNS Responsibilities

Data Feeds

Group Financial Crime is responsible for determining the data attributes that are required to be included in the data feeds to GNS and to inform PIAS of the data requirements which are documented in the GNS Global Standard Configuration document.

PIAS is responsible for the quality and completeness of their data feeds with the PIAS’ 2nd line of defence providing local assurance that the content of the data feeds meets the requirements provided by Group Financial Crime.

PIAS is also responsible for informing GNS Business Support team where:

- an existing system is updated to include additional data items that are in the GNS data requirements, but not previously provided in the data feed (i.e. an updated data feed)
- a new system is developed that holds customer and third-party data that requires screening through GNS (i.e. a new data feed)
- a customer portfolio or additional business is acquired which has individuals or entities that require screening through GNS (i.e. an additional data feed)

PIAS, with the help and support of Group IT and GNS Business Support team, are responsible to ensuring that all remedial actions are completed where a data feed fails or is incomplete so that the missing data can be screened if deemed appropriate. Any remedial actions which do not result in screening being performed as expected, must be reported to Group Financial Crime.

Matching Rules

Matching rules are designed to interrogate the name and other supporting data attributes (e.g. date of birth) to identify potential matches between the PIAS data loaded onto GNS and the list data being screened against.

GNS Business Support team is responsible for the matching rule sets that are used in GNS. PIAS may request additional rule sets, or that certain screening does not take place based on local regulation. All changes to the defined lists screened as detailed in the GNS Standard Configuration document must be approved by Group Financial Crime and GNS Business Support team.

GNS Business Support team is responsible for a regular review (at least every 24 months) of the effectiveness of the screening processes. PIAS is responsible for determining whether there are any local screening test requirements over and above what is included in the GNS Business Support team review. Where there are additional requirements, PIAS must provide details to GNS Business Support team to incorporate in the testing.

9 Transaction Monitoring

In order to identify transactions that may indicate that an associated person has been involved in money laundering and/or terrorist financing related activities, PIAS examines, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions.

'Transactions' includes activity involving customers and non-customers (e.g. suppliers, intermediaries, employee, etc.), payments into and out of the organization, and other means of transferring value (e.g. share transfers, provision of vouchers/credits, transfer of asset ownership; etc.).

9.1 Documented Transaction Monitoring Framework

PIAS monitors transactions related to its activities on an ongoing basis to help identify unusual activity which may be connected to financial crime.

The transaction monitoring framework is designed to regularly monitor the transactional activity of customer and counterparty relationships to ensure that it is consistent with the business' expectations, based on information obtain both at the outset and throughout the relationship. Similarly, the framework also considers supplier, employee and other internal transactional activity.

The transaction monitoring framework must be documented as part of the financial crime operating model, approved by the 'Designated Individual' and reviewed on at least an annual basis. As a minimum, it must include details of:

- which transactions will be monitored
- which financial crime risks transactions are being monitored for
- the anomalies or type of unusual transactions that needs to be identified
- the method of monitoring (automated, manual, or a combination of both)
- the timing of monitoring (real time or post-event)
- the rules, thresholds, scenarios, logic, etc. being applied
- accountabilities and responsibilities for all stages of the monitoring process (including any outsourcing or shared service processing)
- quality checking and assurance processes, including how effectiveness will be measured

The transaction monitoring framework must be approved by PIAS Risk Committee for financial crime.

9.2 Transaction Monitoring Scenarios – AML/CFT

PIAS identifies and documents scenarios relevant to their business, location and products/services that may be indicative of money laundering or terrorist financing. These scenarios will inform the extent and nature of transaction monitoring.

As a minimum, PIAS considers the following scenarios and identifies what (if any) transactional activity will be monitored to detect these scenarios:

- money laundering and terrorist financing threats, typologies and examples identified in local national risk assessments, law enforcement publications or regulatory guidance
- typologies identified by international organizations, such as Financial Action Task Force
- early and voluntary termination of policy to receive surrender value (or redemption) of policy (regardless of any early exit fee)
- cancellation of policy during cooling off period resulting in refund of premiums
- overpayment on policy and subsequent request for refund
- frequent payments on account outside of expected activity i.e. frequent top up payments on medium to long to term policies/investments
- purchase of policies with large lump sum where smaller periodic payments are expected
- payments to third parties with no apparent links to the customer
- indirect customer payments received via distributors

- payments to/from high risk industries i.e. cash intensive businesses etc.
- transaction to/from jurisdiction associated with high risk of financial crime
- payment on account received from overseas
- transaction involving cash or cash equivalent i.e. cashier cheques, money orders etc.
- unexpected change to beneficiaries whom appear unconnected
- customer request to change or increase the sum insured and/or the premium payments are unusual or excessive
- purchase of policies with premiums consider beyond the customer apparent means
- request for payment in different currency to currency used to pay premiums
- regular claims on policy, particularly in quick succession of opening account, including those accounts where a history of fraudulent claims has been identified
- customer borrows against surrender value of policies
- be aware of the external TF risk environment, including geographies with heightened TF risks, emerging typologies and common payment methods used
- take into account the extent of PIAS TF risk exposure, including the size of PIAS business, nature and complexity of PIAS business model or transactions, as well as the geographical base of their customers
- be vigilant against potential financing of other existing or new terrorist groups regionally and globally
- be reminded of new and emerging international typologies in which TF can be financed, including through ransomware, arts and antiquities, and online crowdfunding mechanisms

Scenarios must be based on the businesses risk profile, taking into account the output from relevant financial crime risk assessments, and the above minimum scenarios will only act as an aide memoire to assist in documenting the Transaction Monitoring framework.

9.3 Identifying Relevant Transactions – AML/CFT

PIAS uses identified money laundering and terrorist financing scenarios to identify and document transactions for monitoring.

At a minimum, PIAS seeks to identify transactions that are deemed to pose a higher risk of money laundering and introduce suitable monitoring. Examples include but are not limited to:

- payment of surrender value shortly after policy/account establishment
- customer refunds
- excessive payments received outside of the expected customer activity
- large payments or withdrawal
- numerous small, interlinked payments or withdrawals outside of the expected customer activity
- payments to/from unconnected or unnecessary third parties
- payments to/from distributors
- payments to/from Very High Risk and High Risk rated countries
- overseas payment on an account
- cash or cash equivalent payments i.e. cashier cheques, money orders etc.

- payments to/from customers who are PEPs/RCAs
- payment to/from high net worth individuals
- payments made or received in various currencies
- multiple claims payment in a short period of time
- nature of a transaction (e.g. abnormal size for that customer or peer group);
- the parties concerned (e.g. a request to make a payment to or from a person on a sanctions list).

The above are only examples of potentially higher risk transactions and must not be considered as the only examples relevant for each business. An assessment must be undertaken to determine the relevant transactions.

Transaction monitoring for AML/CFT must form part of the Transaction Monitoring framework which must be approved by PIAS Risk Committee for financial crime.

10 Suspicious or Unusual Activity Reporting – Internal

PIAS reports all internal suspicious or unusual activity reporting relating to AML/CFT, bribery or corruption, fraud or tax evasion.

A transaction is suspicious when it is inconsistent with the customer's known legitimate business or personal activities. Suspicious activity may occur at the onset of the business relation or after the business relation has been initiated.

Employees are trained during induction, as well as periodic email reminders, on the steps to take for reporting suspicious or unusual activity. If an employee or representative finds a transaction may be connected with money laundering or terrorism financing, bribery & corruption, fraud or tax evasion, he/she shall immediately refer the matter to PIAS' Designated Individual, who is PIAS' Head of Risk & Compliance. Alternatively, he/she can send an email to the Risk & Regulatory team at pias.compliance@singlife.com.

The procedures for internal reporting have no requirement for an incident to be proven before it is escalated internally. The threshold for internal reporting is where there is either knowledge, suspicion or reasonable grounds for knowing or suspecting. In cases of doubt, the presumption is to report, rather than not reporting.

10.1 Reporting and Investigation – Money Laundering and Terrorist Financing

PIAS ensures that there are appropriate procedures, systems and controls in place to ensure all employees report in a timely manner information that comes to them in the course of business if they have:

- knowledge;
- suspicion; or
- reasonable grounds for knowing or suspecting

that a person is engaged in, or attempting, money laundering or terrorist financing. This includes the acts of PIAS' actual and proposed customers, employees and other third parties connected to PIAS.

Internal reports are submitted to PIAS' appointed nominated officer or to a delegated person(s)/team.

10.2 Mandatory Reporting – Money Laundering and Terrorist Financing

PIAS identifies any local legal or regulatory reporting requirements in addition to those outlined above (section 10.1). For example, some jurisdictions require reporting of cash transactions above a specific threshold, or transactions with certain jurisdictions, regardless of any knowledge or suspicion of money laundering or terrorist financing.

Where any such requirements are identified, PIAS ensures that there are appropriate procedures, systems and controls in place to ensure all employees report such events to the relevant appointed nominated officer.

10.3 "Tipping Off" Offence

PIAS operates appropriate procedures, systems and controls to ensure that employees do not do or say anything that might "tip off" another person that an internal or external report of (suspected or actual) money laundering or terrorist financing has been made. Additionally, PIAS has appropriate procedures to ensure employees do not otherwise prejudice a money laundering/terrorist financing investigation, even where an internal or external report has not been made.

This must include consideration of the following:

- suitable training and awareness for all relevant employees
- controls over access to internal and external reports
- specific reminders to employees at the time of submission of an internal report
- prepared statements/scripts for customer communication
- handling of customer contact by specialist employees

"Tipping off" does not include disclosures to regulators/supervisors, other PIAS employees and in certain circumstances other financial institutions that are connected to the customer/transaction/activity. In any cases of doubt, the matter must be referred to PIAS' nominated officer who may then escalate to Group Financial Crime team, where appropriate.

11 Suspicious or Unusual Activity Reporting – External

PIAS ensures that internal reports identifying potential money laundering and/or terrorist financing are reviewed, investigated and if necessary, reported externally in a timely manner, having considered both the proceeds of crime and other regulatory requirements.

Suspicion of money laundering will trigger a requirement to submit a money laundering suspicion report (e.g. Suspicious Transaction Report (STR)). The completion of a full and accurate STR to report suspicions of money laundering is a strong indicator that PIAS understands the risks relating to the laundering of the proceeds of crime and our legal and regulatory reporting obligations.

PIAS is encouraged to share additional information or useful insights to existing cases with Law Enforcement Agencies. For example, through the filing of supplementary STRs.

11.1 Review & Investigation of Internal Reports to Determine any External Reporting Requirement

PIAS maintains and operates procedures for the review and investigation of internal reports of financial crime, or suspicions of financial crime, with a view to complying with all external financial crime reporting requirements.

The review, investigation and decision-making process for each internal report received must be documented, including recording the number of reports (by risk type) and the rationale for making, or not making, an external report.

The nature of the review, investigation and decision-making process is determined by PIAS, taking into account its size, number of reports expected, legal and regulatory obligations, industry guidance and law enforcement practices. Separate processes may be necessary for different financial crime risk types.

11.2 Review and Investigation of Internal Reports – Money Laundering and Terrorist Financing

The nominated officer for PIAS is responsible for determining whether the internal reports received amount to ‘knowledge’, ‘suspicion’ or ‘reasonable grounds to suspect’ potential or actual money laundering or terrorist financing. It is the responsibility of the nominated officer (or an appropriate delegate) to consider all internal reports on its own merit and must have access to any information considered relevant to the investigation.

Where knowledge or suspicion is identified (or other local reporting requirements are triggered), a suspicious transaction report (STR) must be prepared and reported to the Suspicious Transaction Reporting Office (“STRO”) as soon as reasonably practicable, and without undue delay.

The nature of the review, investigation and decision-making process is determined by PIAS, taking into account its size, number of reports expected, legal and regulatory obligations, industry guidance and law enforcement practices.

The review and investigation of suspicious activity reports must be fully documented, including:

- record of the number of internal reports received
- record of the number of external reports made
- details of the reason for suspicion (or reason for discounting suspicions)
- details of all enquires made in respect of the review of the internal report
- the reasons why a suspicious activity report was, or was not, submitted
- any communications with authorities in relation to the suspicious activity report

As part of any investigation, the nominated officer may initiate a root cause analysis of the suspicious activity to determine any lessons to be learnt and whether any changes to systems, controls, policies and procedures are required to minimize the likelihood of such an incident reoccurring. This may include re-visiting the money laundering risk assessment for the customer/customer type, product, business line or process and undertaking deep dives into specific aspects of the incident. It may also result in the customer risk rating being increased and due diligence relating to a customer being reviewed/refreshed.

In addition, a STR relating to a high-risk customer or a PEP/RCA must be referred to the relevant MLRO (or equivalent) or a nominated deputy before an external report is made.
Documentary evidence of any such review following review of an internal report must be maintained in accordance with the record retention and retrieval requirements set out in section 16.

11.3 External Reports – Money Laundering and Terrorist Financing

Where it is identified that an external disclosure is required, PIAS follows the requirement set out in local law/regulation/guidance to determine where and how to report and to identify relevant reporting templates, classification codes, submission portals, etc.

In all cases, the nominated officer (or appropriate delegate) must ensure that all external reports contain clear, concise and complete information and must explicitly state the reason for suspicion.

PIAS also records the number of internal reports received and external reports made relating to:
- terrorist financing
- money laundering (total)
- money laundering arising from confirmed fraud (against PIAS)

11.4 Transaction Approvals (‘Consent’ or ‘Defence Against Money Laundering’)

PIAS’ nominated officer must identify if there are local legal or regulatory restrictions in place for seeking law enforcement approval for transactions or other customer activity where suspicions of money laundering or terrorist financing are identified in advance of the transaction/activity. Where

such restrictions are identified, documented procedures are put in place to manage the process for seeking approval and actioning the response.

PIAS ensures that there are safeguards in place to ensure that funds remain blocked (where appropriate) or the transaction is not completed pending decision from the relevant body.

12 Compliance Monitoring

PIAS has a risk-based compliance monitoring plan annually to assess compliance with relevant financial crime laws and related financial crime procedures.

The scope, nature and frequency of monitoring will be documented as part of the FCRMP, considering any local regulatory requirements for regular independent assurance.

The monitoring programme is in addition to quality control activities conducted as part of normal business operations to confirm that controls are being operated (e.g. ongoing checks on the completeness of CDD).

PIAS ensures that the compliance monitoring function has the appropriate resource and capability (knowledge, skills and independence) to effectively oversee and challenge the business in relation to financial crime issues.

The findings of the monitoring programme will be reported to the Head of Risk Management and Compliance and PIAS risk Committee.

PIAS also ensures that prompt remedial action is taken to resolve identified financial crime control weaknesses.

Compliance Monitoring – Resources

The Risk & Regulatory team must have the appropriate resource and capability (knowledge, skills and independence) to effectively oversee and challenge PIAS in relation to financial crime issues.

The Risk & Regulatory team must have full, free and unrestricted access to all business activities, records, data, property and personnel necessary to complete their work.

The Risk & Regulatory team is specifically responsible to oversee compliance of the financial crime activities.

Any identified gaps in capacity, capability or access will be referred to the PIAS Risk Committee and notified to the Group Financial Crime.

In the absence of suitable internal resource, or if otherwise considered necessary by the designated individual or Group Financial Crime, PIAS may seek external verification or assurance of the effectiveness of AML/CFT procedures.

Compliance Monitoring - Findings and Remediation

The findings from any financial crime compliance monitoring review are fully documented and reported to the designated individual(s) and to PIAS Risk Committee.lind

Any identified issues are included within Metricstream (or other operational risk system where Metricstream is not available) along with appropriate action plans and assigned owners to support closure.

Both 1st and 2nd lines of defence are expected to take all appropriate action to remedy any deficiencies identified through compliance monitoring reviews and report on the progress of such activities to PIAS Risk Committee.

13 Financial Crime Training and Awareness

The Head of Risk Management & Compliance will ensure that all employees acknowledge and commit to PIAS' approach to financial crime risks. Training is provided (as part of their induction) through the Essential Learning course, where existing and new employees, permanent or temporary contract workers, including contractors are tested yearly. Employees are reminded any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly through the Group's disciplinary procedures. Where additional training is required for department at high risk of financial crime, tailored training will be provided.

14 Management Information

PIAS follows the Group required suite of key risk indicators and information to monitor the changing financial crime risk profile of the business. This includes but is not limited to information on number and nature of transaction alerts flagged for review/investigations, number of fraud incidents reported, CDD backlog (if any), trends observed from transaction monitoring etc.

The Management Information is presented to the Group Financial Crime monthly, using the Group Financial Crime MI pack conforming to the format, template and requirements set by the Group Financial Crime.

15 Record Retention and Retrieval

PIAS will implement procedures, systems and controls to enable relevant financial crime records to be retained, retrieved and if necessary, deleted to comply with local legislation and PIAS' Records Retention Guidelines. All financial crime related records will be accurate, legible, auditable and retrievable including:

- documents and information obtained to satisfy CDD requirements (e.g. identification documents/certificates, proof of address, EDD documents etc.)

- records relating to customer transactions
- documents relating to the review/investigation of potentially suspicious or unusual activity
- records relating to training (i.e. date of completion, nature of training, attendance records etc.) and compliance monitoring (i.e. reports to senior management)
- records of screening and potential match investigation
- risk assessments and FCRMP documents
- incident investigation reports

PIAS shall ensure compliance with the record retention period as set out in paragraph 10.3 of the MAS FAA Notice 06 on Prevention of Money Laundering and Countering the Financing of Terrorism -Financial Advisers ("FAA-N06").

- For customer due diligence information relating to the business relations and transactions undertaken in the course of business relations, as well as policy files, business correspondence and results of any analysis undertaken, a period of 7 years following the termination of such business relations; and

- For data, documents and information relating to a transaction undertaken in the course of business relations, including any information needed to explain and reconstruct the transaction, a period of 7 years following the completion of the transaction.

PIAS may retain data, documents and information as originals or copies in paper or electronic form or on microfilm, provided that they are compliant with the requirements of the Evidence Act 1893 and Electronic Transactions Act 2010 and are admissible as evidence in a Singapore Court of Law.

PIAS shall retain records of data, documents and information on all its business relations with, or transactions undertaken in the course of business relations for, a customer pertaining to a matter which is under investigation, or which has been the subject of a Suspicious Transaction Reporting ("STR"), in accordance with any request or order from Suspicious Transaction Reporting Office or other relevant authorities in Singapore. In such cases, all relevant records should be retained such that:

(a) any individual transaction undertaken in the course of business relations can be reconstructed (including the amount and type of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity.

(b) the Authority or other relevant authorities in Singapore and the internal and external auditors are able to review business relations, transactions undertaken in the course of business relations, records and CDD information; and

(c) the Group or relevant business entity can satisfy, within a reasonable time or any more specific time period imposed by law or by the requesting authority, any enquiry or order from the relevant authorities in Singapore for information.

The PIAS's retention policy is to keep the documents, which are required by law or regulations, for a minimum of 7 years.

16 Access to Customers' Personal Data

PIAS provides the customer with the right to access their personal data that is in the possession or under the control of PIAS. In addition, subject to section 22 of the Personal Data Protection Act 2012, customers may correct an error or omission in relation to their personal data, provided PIAS is satisfied that there are reasonable grounds for the request.

For the purposes of complying with MAS FAA-N06, PIAS will not be required to provide an individual customer, beneficiary of a life insurance policy, an individual appointed to act on behalf of a customer, a connected party of a customer or a beneficial owner of a customer with:

a) Any access to personal data about the individual that is in possession or under the control of PIAS
b) Any information about the ways in which the personal data of the individual has been or may have been used or disclosed by PIAS
c) Any right to correct an error or omission of the personal data about the individual that is in the possession or under the control of PIAS

For the purposes of complying with MAS FAA-N06, PIAS may, whether directly or through a third party, collect, use and disclose personal data of a customer, beneficiary of a life insurance policy, an individual appointed to act on behalf of a customer, a connected party of a customer or a beneficial owner of a customer, without the respective individual's consent.