PROFESSIONAL INVESTMENT ADVISORY SERVICES

Anti-Bribery and Corruption (“ABC”) 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/ Frankie Tan	PIAS Risk Committee
01/09/2022	2	Annual review	Tang Ming Yang / James Tan	PIAS Risk Committee
10/11/2023	2.1	Annual review	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee
29/11/2024	2.2	Annual review	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee

TABLE OF CONTENTS

1 Overview

1.1 Applicable Legislations

Professional Investment Advisory Services Pte Ltd ("PIAS") is committed to ensure compliance with Singlife Group Financial Crime Policy, Anti-Bribery and Corruption Policy and all applicable regulations that may be issued by the relevant authorities in Singapore.

The applicable regulations for Anti-Bribery and Corruption Policy are the Prevention of Corruption Act 1960 ("PCA") and Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA").

Frequency
This policy shall be kept up-to-date and reviewed annually, or when a material event occurs, whichever is earlier.

1.2 Group Financial Crime Policy

PIAS has a legal, moral and social responsibility to its customers, shareholders and employees to deter and detect those who seek to use our systems to facilitate financial crime. Violations of laws and regulations relating to financial crime may result in criminal, civil or regulatory penalties for Singlife Group, its directors and employees.

PIAS has zero tolerance for financial crime which includes bribery and corruption, facilitation of tax evasion, money laundering and terrorism financing, internal and external fraud, market abuse and economic sanctions violations. Violations of financial crime laws and regulations may result in criminal, civil or regulatory penalties for Singlife Group, its directors and employees.

Financial crime includes:
- Bribery and Corruption;
- Economic Sanctions Violations (including Proliferation Financing);
- Internal and External Fraud;
- Money Laundering and Terrorist Financing; and
- Facilitation of Tax Evasion.

PIAS is committed to comply with the Group's Financial Crime Policy and its relevant guidelines, procedures and risk preference statements and seeks to ensure that its businesses, products and services are not misused for the purpose of money laundering, terrorism financing, sanctions, bribery and corruption, facilitation of tax evasion and fraud events.

PIAS strictly prohibits its directors, management, employees and financial adviser representatives from engaging in acts of financial crime and will investigate and support prosecution, where

appropriate, of those who are involved. PIAS reserves the right to reject any customers, payment, or business(es) that is not consistent with Group's risk preference statements and aims to continuously strengthen their processes to ensure compliance with applicable laws and regulations.

Any waiver or deviation from this policy requires approval by Senior Management on reasonable grounds and needs to be in line with the Group Financial Crime Policy and all applicable regulations.

1.21 Reporting on Waiver/Deviation to Group Financial Crime

Any non-compliance with the policy must be immediately reported to PIAS CEO and PIAS Head of Risk Management & Compliance ("RM&C") stating the nature and reasons for the non-compliance. PIAS CEO and PIAS Head of RM&C will escalate incidents of non-compliance to the Group Head of Legal & Compliance as soon as possible, together with a remediation action plan.

1.3 Top-Level Commitment

PIAS Senior Management promotes an ethical and compliant culture to deter acts of financial crime. This includes enhancing awareness and reinforcing understanding of employees' personal responsibilities under the Group's Business Ethics Code and promoting an ethical and compliant culture in third parties that are carrying out, retaining or obtaining business on behalf of PIAS.

PIAS Senior Management sets the 'tone from the top' by communicating Group's approach to financial crime in line with Financial Crime Risk Preference Statements and Group's Business Ethics Code at least annually. Such communication shall explain Group's approach to financial crime; explain the consequences of breaching Group's standards; contain a commitment to carry out business fairly, honestly and openly; information on how to report financial crime; highlight mechanisms for confidentiality raising concerns through whistleblowing (e.g. Group's 'Speak Out Charter' programme); local regulatory requirements; promote a culture that financial crime is not acceptable.

The evidence of communication of the 'tone from the top' will be retained for at least 7 years.

1.4 Risk Preference Statements

PIAS aligns its internal risk appetite, and supporting policies, procedures and practices to Group's Financial Crime Risk Preference Statements as follows:

Bribery and Corruption

Definition

1.41 Corruption is defined as an act of receiving, asking for or giving any gratification to induce a person to do a favor with a corrupt intent. It may include money, sexual favors, properties, promises and services.

1.42 Bribery is defined as an act of corruptly authorizing, giving, agreeing to give, promising, offering, soliciting, receiving, or agreeing to receive any gratification.

1.43 Facilitation payment is a payment made to secure or expedite the performance by a person performing a routine or administrative duty or function.

1.44 Kickbacks are typically payments made in return for a business favor or advantage.

PIAS has no appetite for acts of bribery or corruption by an employee (inclusive part-time, temporary or full-time basis), contractors, consultants, vendors, service providers and any other agencies or third parties associated with PIAS. This would include:

I. Active bribery (the giving of a bribe or inducement);
II. Passive bribery (the receiving of a bribe or inducement); and
III. Facilitation payments or inducements to or from public officials the payment of inducements to public officials by an employee or Financial Adviser Representative or providing facilitation payments.

PIAS has limited appetite for gifts, hospitality or entertainment received or offered by an employee or Financial Adviser Representative.

Group seeks a continually improving trend on instances of fraud loss or acts of dishonesty.

1.5 Employee Culture

The Head of Risk Management & Compliance [“RM&C”] shall ensure that all employees acknowledge and commit to Group’s approach to financial crime risks via annual attestation to Business Ethics Code upon completion of Learning Management System / Essential Learning Course. The annual attestation and Learning Management System / Essential Learning Course are applicable to existing and new employees, permanent or temporary contract workers including contractors. They are reminded that any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly through the Group’s disciplinary procedures.

In addition, in areas where there is higher risk of exposure to financial crime (for example through the Enterprise Wide Risk Assessment (EWRA) or occurrence of risk events), PIAS will consider to issue additional internal communications as part of an ongoing training and awareness programme.

Communication from Group Financial Crime is also available on Group's Business Ethics Code and Employee Handbooks.

The evidence of acknowledgement of the Code will be retained by PIAS for at least 7 years.

1.6 Third Party Culture

Where third parties are carrying out, promoting, obtaining or administering business on behalf of PIAS, the function managing the third party relationship will take reasonable steps to ensure that the third party understands Group's approach to financial crime risks and has implemented appropriate procedures to mitigate these risks to PIAS.

PIAS will encourage all suppliers to sign up to the Supplier Code of Behaviour, where the supplier commits to complying with all applicable financial crime laws and regulations.

The Singlife legal counsel will ensure that the contract clauses, terms and conditions, statements of work, or other formal communication with those individuals or businesses acting on behalf of PIAS, includes references to Group's approach to financial crime.

In addition, where PIAS identifies areas as being higher risk or exposure to financial crime, PIAS will consider issuing additional external communications to embed Group's approach to financial crime risk and consequences for non-compliance as well as raise awareness of expected Group financial crime compliance standards / procedures / controls. The additional communications will demonstrate senior management commitment on the prevention of financial crime and reassure existing and prospective associated persons.

The evidence of communication to third parties and their formal acknowledgements (where applicable) will be retained for at least 7 years.

1.7 External Communications

The Head of Risk Management & Compliance identifies and documents any local regulatory or legal requirement for public disclosure of PIAS' approach to managing their financial crime risks.

2 Governance & Accountabilities

2.1 Risk Governance

PIAS Risk Committee is responsible for ensuring a strong and effective compliance culture is in place for the deterrence of financial crime activities.

PIAS is to ensure that business processes are robust and there are adequate risk mitigating measures in place. PIAS should:

a) receive sufficient, frequent and objective information to form an accurate picture of the financial crime risks including emerging or new ML/TF risks which PIAS is exposed to through its activities and business relations;

b) receive sufficient and objective information to assess whether controls are adequate and effective;

c) receive information on the legal and regulatory developments and understand the impact these have on the financial crime risk management framework; and

d) ensure that processes are in place to escalate important decisions that directly impact the ability of the business to address and control financial crime risks, especially where controls are assessed to be inadequate or ineffective.

2.2 Governance Responsibilities

PIAS Risk Committee provides oversight on management of financial crime risk and ensure that any gaps or deficiencies identified from the risk assessment are addressed in a timely manner. PIAS Risk Committee is required to escalate to the Board Risk Committee via the Group Head of Legal & Compliance on any known financial crime breaches, control failures, issues and risks outside tolerance.

In addition, PIAS Risk Committee will review and approve any financial crime policies and procedures as well as approve the approach for training, internal communications relating to financial crime. All public disclosures of matters relating to financial crime risk management (including publication on an external PIAS website) will be approved by Group Financial Crime.

An annual approval of the accountabilities and responsibilities (by PIAS Risk Committee) for PIAS's Designated Individual, the Money Laundering Reporting Officer ["MLRO"] and the Nominated Reporting Officer(s) are required. For PIAS, the Designated Individual and MLRO are the same individual (i.e. the Head of Risk Management & Compliance). The Nominated Reporting Officer is the Risk & Regulatory Team Lead who reports to the Head of Risk Management & Compliance.

2.3 The Three Lines of Defence Operating Model

Roles and responsibilities of Three Lines of Defence

First line of defence (1st LOD): Business, Operations and Other Support Functions

- Financial Adviser Representatives, Operations, Training & Competency, Finance, Partnership Management, People Function, Adviser Maintenance Unit, Business Development and Channel Marketing and Transformation.

Roles and responsibilities include:

- Risk identification, ownership, management and control, including a supportive risk culture
- Executing the requirements of an adequate and appropriate Financial Crime Risk Management Framework [FCRMF]
- Escalations to Group Financial Crime Risk Management and to Business and Risk Executives (including appropriate reporting) where required in a timely, transparent and open manner
- Apply and execute the Group Financial Crime Risk policies as they apply to the Business Area
- Support a resourcing model adequate and appropriate to maintaining a Financial Crime Risk Management Framework
- Develop open communication channels with 2nd LOD to ensure specialist support, advice and guidance is obtained from financial crime compliance experts as required
- Partner with 2nd LOD to design and implement an assurance testing strategy and framework for all financial crime controls
- Ownership of all data
- Undergo annual financial crime training (minimally covering ML/TF) to be aware of the latest trends and developments and the related regulatory compliance obligations

Second line of defence (2nd LOD): Financial Crime Function

- Risk Management & Compliance

Roles and responsibilities include:

<u>Strategy</u>

- Define and implement a Financial Crime Risk Management Framework
- Provide insight, advice and guidance to the Group and Business on current financial crime regulatory, legal and industry challenges

<u>Advisory and Oversight</u>

- Design, implement and maintain a robust financial crime risk management control framework as well as ongoing monitoring of the relevant internal controls
- Monitor and review 1st LOD control adequacy and effectiveness and provide increasing oversight and challenge
- Remediate any non-conforming or ineffective systems and controls in 1st LOD and 2nd LOD
- Provide training and awareness on Financial Crime related matters
- Design and maintain the management information reporting framework
- Support a resourcing model to fulfil the Group Financial Crime Risk Management requirements and provide expert advisory support and guidance to 1st LOD

<u>Policy</u>

- Own and develop appropriate financial crime policies, standards and guidance as to how these should be interpreted and implemented

- Provide oversight, challenge and approval on all exceptions to financial crime policies and standards

Assurance

- Provide advice, guidance and support to 1st LOD Testing and assurance activity

The Risk & Regulatory Team is responsible in alerting the board of directors and/or senior management if there is any reason to believe that the company's officers, employees or financial adviser representatives are failing or have failed to adequately address financial crime risks and there are concerns that PIAS had breached the applicable ML/TF laws and regulations.

While the other support functions also play a role in mitigating financial crime risks, the Financial Crime function is typically the contact point regarding all financial crime related issues for domestic and foreign authorities, including supervisory authorities and law enforcement authorities.
The Group Head of Legal & Compliance is responsible for escalating any material financial crime related risks or regulatory breaches to the Group CEO and to the Board Risk Committee.

Third line of defence (3rd LOD)

- Internal Audit

The Internal Audit function is responsible for undertaking periodic evaluation of the financial crime risk management framework and controls for the purpose of reporting to the Audit Committee. Such evaluations should at minimum cover ML/TF risks to assess:

(a) the adequacy of ML/TF policies, procedures and controls in place for identifying ML/TF risks, addressing the identified risks and complying with laws, regulations and notices;

(b) the level of compliance and effectiveness of the employees, officers and agents in implementing the policies, procedures and controls;

(c) the effectiveness of the compliance oversight and quality control measures including parameters and criteria for transaction alerts; and

(d) the effectiveness of the training of relevant employees, officers and financial adviser representatives.

Roles and responsibilities include:

- Design, implement and maintain an audit plan to evaluate and provide independent assurance on the appropriateness, effectiveness and adequacy of financial crime policies, procedures, standards and financial crime risk management systems and controls
- Maintain the Whistleblowing communication channels

- Provide independent oversight and challenge of 1st LOD and 2nd LOD financial crime risk management control activities

2.4 Financial Crime Programme

The Designated Individual shall put in place an appropriate Financial Crime Programme and ensure compliance with applicable regulatory requirements and Group Financial Crime Policy.

Financial Crime Prevention Programme

- Financial Crime Business Standard Attestation for PIAS (MetricStream or equivalent)
- Annual Financial Crime Risk Assessment using the Group FC template
- Implementation of the Group Financial Crime Policy and Group Risk Assessment action plans
- Review of PIAS Gifts and Hospitality Register and Conflicts of Interest entries
- Bribery and Corruption Detection Checks – Review of Gifts and Entertainment expenses (including sponsorships and donations) in Finance
- Annual reminder to all staff on registering Gifts & Entertainment and Conflict of Interest
- Annual PIAS staff training
- Regular Tone from the top emails on Financial Crime
- 'Speak Out Charter' whistleblowing
- Reporting of fraud incidents in PIAS
- Business Ethics Code (annual staff sign-off)
- Timely resolution of any Financial Crime related audit issues
- Quarterly MI updates for PIAS Risk Committee
- Monthly Financial Crime Management Information submission for PIAS.
- Investigation and reporting of any instances of fraud, bribery & corruption, sanctions, money laundering or facilitation of tax evasion related issues to PIAS and where required escalation to Group Financial Crime.
- Perform risk assessment and report any true matches in Global Name Screening (GNS) for all categories (i.e. sanctions, Politically Exposed Persons) and High Risk / Very High Risk Jurisdiction Index to Group Financial Crime via monthly MI reporting.

Financial Crime Oversight Activities with Business Units

- Financial Crime Training to New Representatives during Induction Training
- Facilitate/ follow up on issues relating to Global Name Screening (GNS), Fraud and Suspicious Transactions Reporting MI review
- Attend to Law Enforcement enquiries, where required

2.5 Review of Financial Crime Risk Management Programme

PIAS will review its 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 instigated where there are significant changes to the business, such as a merger,

acquisition, disposal, major new product line/customer proposition, business transfer/reorganisation, new geographical market, new or revised legislation and/or regulation etc. At a minimum, the review process will be documented at PIAS Risk Committee.

2.6 Notification of Appointments

PIAS will provide to Group Financial Crime details of the individuals appointed as the Designated individual, MLROs (or equivalent) and Nominated Officer (or equivalent).

Details will include the name of the individual(s); the names of the business areas for which they are responsible; date of appointment; confirmation of any regulatory approval required; confirmation of any regulatory notification required.

Notification to Group Financial Crime will occur on any subsequent change to the appointed individuals or their scope of responsibility.

2.7 Appointment of a Designated Individual

The PIAS Risk Committee must identify and appoint a member of the Senior Management as the Designated Individual, who will ultimately be accountable for financial crime risk management in PIAS. For PIAS, the Designated Individual is the Head of Risk Management & Compliance.

Where appropriate, PIAS may appoint additional designated individuals, provided that it is clear who has ultimate accountability for financial crime. All appointments must be approved by the PIAS Risk Committee.

To be able to adequately fulfil the role, the appointed person must:

a) understand the market/business/cell to which they have been appointed and how the financial crime legal, regulatory and internal policy requirements apply
b) understand the level of financial crime risk exposure within their market/business/cell
c) have an appropriate level of seniority, skills, knowledge and experience in implementing, maintaining and monitoring compliance with financial crime standards
d) have sufficient standing to act independently under his/her own authority.

All appointments (including delegations) must be fully documented including details of accountabilities and responsibilities and must be agreed on at least an annual basis by the PIAS Risk Committee.

The CEO (or equivalent) must ensure that the role of 'Designated Individual' is covered at all times. Any gaps in coverage of over 1 month must be reported to the PIAS Risk Committee and Group Financial Crime, together with a plan for resolution.

2.8 Responsibilities of a Designated Individual

At a minimum, the responsibilities of the designated individual for financial crime risk management must include:

a) any local regulatory or legal accountabilities for financial crime
b) active involvement in financial crime risk management, supervision and critical decision-making processes
c) oversight and input into the design and ongoing review of local financial crime policies, procedures, systems and controls
d) being a key member of financial crime governance forums/committees
e) oversight of and involvement in the business/market/cell financial crime risk assessment(s) and reporting process
f) ensuring adequate financial crime resources are deployed to mitigate identified risks
g) demonstrating 'tone from the top' by embedding a culture of compliance, for example, through promotion of a zero tolerance appetite to acts of bribery and corruption by any person associated with PIAS
h) assessing and reporting on the adequacy of the financial crime risk management programme through ongoing testing, management information and board/committee reporting
i) ensuring the relevant local board(s) are adequately informed of internal and external financial crime developments
j) oversight of financial crime related breaches and the provision of feedback to board or equivalent on levels of compliance

The designated individual may delegate activities to other competent persons, however, the ultimate responsibility for the management of financial crime risk will remain with the designated individual. The responsibilities of the designated individual must be documented within their role profile or job description.

2.9 Designated Individual Review Process

The on-going appropriateness of the designated individual for financial crime risk must be assessed on a regular basis to ensure they remain appropriate for the role. This must include:

a) assessment through the annual performance management process (including any ad hoc performance issues)
b) consideration of suitability against the wider team's seniority, skills, knowledge and experience
c) evidence of continued senior management financial crime training and/or attendance at relevant financial crime events.

3 Risk Assessment

3.1 General Principles and Risk Assessment

In general, PIAS shall undertake periodic risk assessment to identify, analyse, assess and understand, its money laundering and terrorism financing risks in relation to the clients, the countries and jurisdictions the clients are from or in, and the products, services, transactions and delivery channels of PIAS.

PIAS shall document the risk assessment and consider all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation.

PIAS shall exercise adequate due diligence when dealing with clients, natural persons appointed to act on the clients' behalf, connected parties of the clients and beneficial owners of the clients. This includes companies with bearer shares where identities of bearer shares must be made known to PIAS, and when there are changes to the ownership of these shares or named custodian.

Policies, procedures and controls must be properly developed, implemented and approved by the Senior Management to manage and mitigate the risks identified.

Where higher risks are identified, there should be enhanced measures and controls to mitigate these risks. The performance of the controls shall be reviewed on an annual basis for its effectiveness.

3.2 Enterprise-Wide Risk Assessment ("EWRA")

PIAS takes appropriate steps to identify, assess and understand its financial crime risk (or minimally the ML/TF risks) at the enterprise-wide level. The assessments for PIAS will be consolidated by Group so that the financial crime risks exposure may be evaluated. 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 are documented and approved by PIAS senior management even if there are no significant changes to the enterprise-wide risk assessment. PIAS must give full support and active cooperation to the Group's enterprise-wide ML/TF risk assessment.

The assessment should 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.

3.3 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 where the customers are from or in;
- the countries or jurisdictions of operations; and
- the products, services, transactions and delivery channels

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 senior management and shared with the Board. Thereafter, the risk assessment information may be provided to the Authority upon request.

3.4 Product Developments, Practices, Technologies and Customer Proposition Initiatives

On a regular basis (at least annually), PIAS risk-assesses each active product and/or service offering to identify its susceptibility to financial crime. The assessment may group products/services into categories or product sets where appropriate (e.g. all pension products may be assessed together), provided the full product/service offering is included.

This assessment considers all financial crime risk types and is carried out in such a way as to facilitate the identification and implementation of suitable mitigating controls.

An assessment of the risks associated with new product developments, new business practices, including new delivery mechanisms, the use of new or developing technologies for both new and pre-existing products, amendments to existing products and customer proposition initiatives are undertaken in line with Group's requirements. As part of this, the Head of Risk Management & Compliance will ensure that consideration of financial crime risks forms part of the new product development process.

All assessments of risk required under this section is documented including all assessment steps taken. All new product types, new business practices including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products or new customer proposition initiatives assessed by the Risk & Regulatory Team are notified to Group Financial Crime as part of the 'matters for escalation' submission.

Where any new product or customer proposition initiative is outside of PIAS's existing business model/product range (e.g. introduction of life products to a GI business), or introduces significant new risks (e.g. a high risk product or a new country of operation), the Head of Risk Management & Compliance will present the proposal and the risk assessment to Group Financial Crime prior to the new product or customer proposition going live.

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

3.5 Mergers and Acquisitions

The Head of Risk Management & Compliance ensures that an assessment of the financial crime risks associated with mergers and acquisitions (including acquisitions of portfolios of customers from other financial services firms) is undertaken in line with the requirements of Group's mergers and acquisitions processes.

The risk assessment will be documented and consider the risks arising in both:

- **merger/acquisition process** – particularly whether there are increased bribery and corruption risks associated with the merger/acquisition (e.g. through engagement of third-parties, negotiators, etc, as a result of the jurisdiction involved, due to secrecy in the process, etc)

- **acquired business** - the extent to which the acquired customers, products, services, employees, locations, systems, data, etc. introduce additional or different financial crime risks to the acquiring Singlife business especially where the firm's processes and procedures are below the requirements of Group's Standards

PIAS will consider whether any sample testing of key financial crime prevention processes and procedures (such as customer due diligence activities or sanctions name screening) needs to be undertaken as part of the risk assessment.

After reviewing the risk assessment, PIAS will put in place appropriate action plans to ensure all financial crime deficiencies identified in the risk assessment are remedied and implement suitable controls to manage the financial crime risks in line with Group's financial crime risk appetite and tolerances in both the transition/acquisition process and in the 'new' business.

3.6 Risk Based Controls

The Head of Risk Management & Compliance will uses EWRA and any other assessments of financial crime risk to design, implement and operate effective and proportionate controls to mitigate financial crime risks.

A risk-based approach is most likely to be taken in respect of the extent, nature and frequency of controls relating to:

- Customer due diligence (including enhanced due diligence and associated person (non-customer) due diligence)
- Screening
- Ongoing monitoring
- Compliance monitoring
- Training

The risk-based approach will be documented (either as a stand-alone document or incorporated in other relevant documents) and take into account of Financial Crime Policy.

The approach will be reviewed at least annually to ensure continued suitability.

4 Due Diligence

4.1 Customer Due Diligence

Customer Due Diligence ("CDD"), Simplified Customer Due Diligence ("SCDD") or Enhanced Customer Due Diligence ("ECDD") is performed on all customers to the required level as determined by Group Financial Crime Policy. This is to comply with regulatory requirements to 'Know Your Customer' and to ensure that the business knows who it is dealing with. This includes customers, employees, business partners and third-party providers.

Appropriate control mechanism is in place to ensure compliance with the relevant regulatory requirements relating to CDD, SCDD, ECDD and reliance on third-party providers to conduct CDD.

Broadly, as a safeguard against establishing any business relations or undertaking any transaction, that is or may be connected with or may facilitate ML/TF, the MAS regulations require that the identities of the following persons are identified and verified:

- the customer (individuals, corporates or other body of persons)
- any beneficial owner of the customer
- any beneficiary
- any natural person appointed to act on behalf of the customer
- any connected party of the customer
- any beneficial owner of a beneficiary

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

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

CDD/SCDD/ECDD requirements include provisions for all relevant customer types and include requirements for completing CDD/SCDD/ECDD on beneficial owners where appropriate. The circumstances in which a customer should be subject to enhanced due diligence (ECDD) to reflect a risk assessment or local regulatory requirements are documented in the PIAS' FCRMP.

CDD/SCDD/ECDD will be completed at the commencement of a customer relationship and is kept up-to-date throughout customer relationship.

CDD/SCDD/ECDD evidence is retained and retrievable according to records retention requirements.

The quality, completeness and accuracy of CDD/SCDD/ECDD is subjected to a regular, on-going quality control process, and the nature, frequency and scope of this control process is documented in the FCRMP.

The results of CDD/SCDD/ECDD quality testing form part of business's compliance monitoring and reporting.

For the purposes of this document, 'customer' includes any party where there is regulatory obligation to complete due diligence under AML/CFT legislation and may include relationships referred to as something other than 'customer' (For example 'client', 'insured party', 'policyholder', 'account holder', 'beneficiary', 'contract holder', etc.).

All customers of PIAS are subjected to AML/CFT due diligence requirements.

Risk-based Application of Customer Due Diligence (CDD)

PIAS defines the nature and extent of Customer Due Diligence (CDD) applicable to the business(es).

CDD is conducted according to the level of risk posed by customers:

- Simplified Customer Due Diligence (SCDD) may be applicable in limited and pre-defined reduced risk circumstances;
- 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.

Customers are classified as either Standard Risk customers or High Risk customers. High Risk customers are reviewed annually.

Risk assessment on individual customers ensure that the risks a customer relationship brings to PIAS are duly captured and that an appropriate classification for the customer is established. This will ensure due diligence measures and ongoing monitoring are effective and proportionate.

Timing of Initial Customer Due Diligence Activities

PIAS has procedures in place to complete the initial Customer Due Diligence (CDD) activities for customers before establishing the business relationship.

The approach to local exceptions for timing of CDD are documented and regularly reviewed to ensure compliance with local legislation and regulatory guidance.

Ongoing Customer Due Diligence

PIAS determines the appropriate level of ongoing Customer Due Diligence appropriate for its customers and products, ensuring that the approach taken aligns to its risk appetite and is fully documented as part of the Financial Crime Programme.

On-going Customer Due Diligence 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 Customer Due Diligence 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 the appropriate classification is assigned to the customer
- ensure that the customer and their activities remain within Group's risk appetite

On-going Customer Due Diligence is done annually and on a trigger event basis.

Periodic Reviews

High Risk Customers
All customers identified as 'high-risk' are reviewed on an annual basis.

Corporate Customers
Periodic reviews are done every 5 years for corporate customers 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 on customers shall be performed for cases/or instances where there is:

- identification of a credible involvement in financial crime
- increased risk of customer being involved in ML/TF or other financial crime (e.g. through relevant alerts from the transaction monitoring system, court production order or unexplained wealth orders)
- where a suspicious activity report relating to the customer has been filed
- becoming aware of facts or information which leads to doubt over the veracity or adequacy of the due diligence previously obtained
- becoming aware of a change in the individual customer's country of residence

- becoming aware of a change in beneficial ownership of a corporate customer
- becoming aware of a change in the customer's nature of business;
- identification of a PEP, or an increase in the risk rating of an existing PEP
- becoming aware that the customer no longer qualifies for Simplified Customer Due Diligence (e.g. through the loss of regulatory or listed status or selection of a new product)

The nature of ongoing due diligence is 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 is 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.

4.2 Associated Persons and Non-Customer Due Diligence

PIAS completes risk-based Due Diligence ("DD") on non-customer relationships to the required level as determined by Group Financial Crime Policy and FCRMP. This includes employees, third-parties, intermediaries, suppliers and other relevant parties (e.g. Joint Venture Partners). This is to ensure that the business knows with whom it is dealing, particularly to mitigate sanctions and bribery risks.

- the nature, extent and format of DD will be risk-based to reflect the level of financial crime risk. This will take into account the role the associated person is undertaking for PIAS and the jurisdiction involved
- the nature, extent and format of DD will be documented, communicated and accessible to relevant parties
- the circumstances in which an associated person should be subject to additional due diligence to reflect a risk assessment or local regulatory requirements will be documented in PIAS' FCRMP
- DD will initially be completed at the commencement of a relationship and will be kept up to date throughout the relationship according to a schedule determined in PIAS' FCRMP.
- DD evidence will be retained and will be retrievable
- quality, completeness and accuracy of DD will be subject to a quality control process, the nature, frequency and scope of this control process will be documented in the FCRMP
- Results of DD quality testing will form part of PIAS' Compliance monitoring and reporting

4.3 Employees – Recruitment

Singlife's People Function oversees hiring for PIAS. PIAS' new employees (both permanent and temporary, including contractors) are hired objectively and thoroughly screened prior to employment in line with Pre-Employment Screening Guidelines.

This includes an interview process as well as obtaining and verifying any references given and analysing any gaps in employment history in line with the Group Fit and Proper Minimum Requirements. Where declared in the employment application, Singlife People Function ascertains whether the candidate has any conflicts of interest and/or been referred by a public official. Where there is a conflict as a result of referral from a public official, this will be escalated to the 2nd line of defence, Risk & Regulatory Team.

After onboarding the employee, the individual is subjected to appropriate pre-employment name screening by Singlife which will include Sanctions, Politically Exposed Persons ("PEPs") and Special Interest Persons ("SIPs") screening using Global Name Screening tool ("GNS").

4.4 Employees – Post-Recruitment

PIAS ensures that the compensation structure for all employees does not create incentives for inappropriate behaviour that is not aligned to Group's values.

Employees name-screening are screened daily in GNS to detect for PEP, sanctions and adverse news.

PIAS identifies all roles where there is a higher exposure to financial crime risks and, where appropriate, apply additional controls in relation to them and the activities undertaken, such as broader background checks, increased supervision, enhanced training, additional compliance monitoring.

PIAS will consider whether on-going due diligence activities are required for employees where their roles have a higher exposure to financial crime risks.

PIAS requires that all employees attest annually to Group's Code of Business Ethics.

4.5 Intermediary Due Diligence

PIAS determines the additional due diligence activities required, where an intermediary wants to partner with PIAS. This due diligence will be specific to confirming the intermediaries' ability and capability to effectively manage the money laundering and terrorist financing risks, and include:

- obtaining confirmation of the intermediary's regulated status from an official source
- sanction screening and special interest person/entity of the firm and directors

- PEP screening of the directors

Where local legislation permits, PIAS may be able to rely on the identification and verification work completed by the intermediaries introducing the business within the same market.

Where PIAS is able to, and wishes to, place reliance on the identification and verification work completed by the intermediary introducing the business, PIAS will satisfy itself that the intermediary 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 may only rely on third parties to perform customer due diligence on its behalf, if all of the following conditions are met:

(a) PIAS is satisfied that the third party is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate AML/CFT measures in place to comply with those requirements

(b) PIAS has taken appropriate steps to identify, assess and understand the ML/TF risks particular to the countries or jurisdictions that the third party operates in

(c) The third party is not one which have been specifically precluded by the MAS from relying upon; and

(d) The third party is able and willing to provide, without delay, upon request, any data, documents or information obtained by the third party with respect to the measures applied on our customer, which we would be required or would want to obtain.

PIAS also considers the matters shown below before agreeing to rely on the identification and verification information provided by the intermediary:

- the intermediary'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 intermediary's general efficiency in business dealings
- any other knowledge, whether obtained at the outset of the relationship or subsequently, regarding the standing of the intermediary being relied upon

Whilst reliance can be placed on third parties to conduct customer due diligence activities, the ultimate responsibility for compliance with local laws and regulations cannot be outsourced and will be remain with PIAS.

4.6 Non-Employee Associated Persons and Third-Party Risk Management Framework

PIAS ensures that employees responsible for engaging and dealing with non-employee associated persons and third parties (e.g. suppliers of services or intermediaries) are aware of the requirements set out and that accountabilities for compliance with them are clearly documented and understood.

There will a Group-led risk-rating policy applied to non-employee associated persons and third party relationships, which records the status of the relationship, assesses and records the risk of bribery and corruption associated to each relationship. For associated persons providing services "for or on behalf" of Singlife, this data must be stored within an associated person register which records relevant details and establishes appropriate levels of due diligence.

4.7 Non-Employee Associated Persons and other Third Party Due Diligence

Non-employee associated persons and third party due diligence takes place prior to the receipt of goods or services from them. They are screened using GNS before a business relationship is established. Status of the relationship is ascertained and documented.

Where the non-employee associated person is an entity other than a natural person, for example a company, the key corporate personnel and beneficial owners are identified. The key corporate personnel and beneficial owners subject to identification procedures are equivalent to the identification (but not verification) requirements required for a similar entity under the relevant local AML requirements.

4.8 Third Party Screening

Screening of third parties (including non-employee associated persons and identified key corporate personnel and beneficial owners follows the screening requirements of the relevant.

Confirmed true matches as a result of name screening are escalated to Risk & Regulatory Team for advice as to the materiality of the issue and whether the business should proceed with the relationship.

4.9 High Risk Third Parties and High-Risk Non-Employee Associated Persons – Financial Crime Review and Approval (ABC)

Risk & Regulatory Team reviews and assesses the following relationships:

- all 'high risk' non-employee associated persons
- any non-employee associated person or third party which has been linked to bribery and/or corruption

The nature and scope of the non-employee associated person or third-party business relationship will be reviewed by the Risk & Regulatory Team who will recommend to the CEO whether to enter

into the relationship or not, and where necessary determine any additional controls required to mitigate the bribery and corruption risks associated with the third-party are documented.

PIAS will not enter into a business relationship with a high-risk third party unless it has been approved by the Head of Risk Management & Compliance or PIAS CEO. In addition, PIAS Risk Committee must approve the business relationship prior to its commencement.

The decision whether to enter the business relationship with the non-employee associated person or third-party concerned must be fully documented and include an assessment of the bribery and corruption risks associated with the business relationship and the detailed rationale behind the decision made.

Where a non-employee associated person or third-party relationship is rejected for financial crime-related reasons, PIAS must ensure that the name of that third-party is added to any relevant internal watchlist.

4.91 Non-Employee Associated Person and Third-Party Documentation

Contracts with all non-employee associated persons and third parties will contain relevant anti-bribery and corruption representations and warranties as determined by the relevant legal counsel. The legal counsel will ensure that the contract clauses, terms and conditions, statements of work, or other formal communication with those individuals or businesses acting on behalf of PIAS, includes references to Group's approach to financial crime.

All non-employee associated persons and third parties receive Singlife's Supplier Code of Behaviour and all relationships that are determined to be Medium- or High-risk rated sign up to and undertake to comply with the Code.

Copies of due diligence materials, including risk assessments, the results of screening, and any referrals to Risk & Regulatory Team or governance committees are retained and are retrievable. If a non-employee associated person or third party refuses to sign up to ABC contract clauses or the Supplier Code, any proposal for their engagement must be submitted to the Risk & Regulatory Team for review, risk assessment and escalation for approval (if necessary) to PIAS Risk Committee.

5 Screening

5.1 Sanctions Screening

PIAS screens names (customers, employees, third parties etc.), using GNS as the global screening tool to check against sanctions lists.

All customers (including where appropriate, directors, controllers and beneficial owners), counterparties, associated persons (including employees and any other relevant parties identified by PIAS (e.g. Joint Venture partners), are screened using GNS.

The results of screening are used to inform a risk-based decision whether to engage in business with a client, associated person or other third party, or to participate in a business transaction.

To ensure that the PIAS does not deal with any sanctioned individuals and entities, PIAS screens the following persons using the Group-approved name screening tool (GNS) at onboarding and regularly:

- its customers;
- any beneficial owner(s) of the customer;
- any beneficiary;
- any natural person appointed to act on behalf of the customer;
- any connected party of the customer;
- any beneficial owner(s) of a beneficiary;
- any third party the company engages in business with;
- any insured person;
- the company's directors, representatives and employees

The screening is conducted against the financial crime watchlists and sanctions lists including but not limited to those issued by:

- US Office of Foreign Assets Control (US OFAC),
- HM Treasury,
- United Nations Security Council,
- the European Union,
- Monetary Authority of Singapore and
- Singapore Ministry of Home Affairs

If any sanctioned individual or entity is identified, PIAS will action on the following:

a) immediately freeze funds, other financial assets or economic resources of the designated individual and entity;
b) abort entering into any financial transactions or provide financial assistance or services in relation to: (i) designated individuals, entities or items; or (ii) proliferation and nuclear, or other sanctioned activities;
c) inform MAS of any fact or information relating to the funds, other financial assets or economic resources owned or controlled, directly or indirectly, by a designated individual or entity; and
d) file a suspicious transaction report ("STR") and extend a copy to MAS

PIAS clears sanction alerts within 2 business days and ensures the appropriate actions are taken.

5.2 PEPs Screening

PIAS identifies Politically Exposed Persons ("PEPs") relationships in order to appropriately manage the potentially increased money laundering, bribery and tax evasion risks.

Customers (including identified controllers and beneficial owners), counterparties, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture partners) are screened to identify association to financial crime.

Customers (including identified controllers and beneficial owners) and counterparties may be screened to identify association to financial crime. (Note: Any decision not to screen customers/ counterparties/clients are documented and agreed by PIAS Risk Committee).

PIAS clears PEP alerts within 10 business days and ensures the appropriate actions are taken.

All PEPs are classified as high-risk customers. Prior to forming any business relationships with the PEPs, approval is sought from the CEO. Thereafter, they are monitored as part of PIAS' High-Risk Customers list.

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

PIAS uses GNS as the standardized screening tool. Dow Jones also provides media reports to identify individuals and entities with a documented implication of relevant criminal activity including corruption, financial crime, trafficking, organised crime, terror and tax crime. Where considered necessary (e.g. when completing enhanced due diligence), additional supplemental resources may be used, such as internet media searches or specialist external due diligence reports.

5.4 State-Owned Companies (SOC) Screening

Being able to identify a connection or relationship with a state-owned company, or a state-owned company 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.

Screening of SOC is performed using GNS and 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 will be included within the relevant enhanced due diligence records.

5.5 Additional Screening

PIAS identifies and manage the financial crime risk inherent in entities and individuals with which PIAS may have dealings.

PIAS screens customers (including where appropriate their key corporate personnel and beneficial owners), counterparties, associated persons (including employees) and any other relevant parties identified by PIAS (e.g. Joint Venture Partners) to identify exposure to:

- jurisdictions with an increased financial crime risk
- parties identified as linked to financial crime

PIAS uses the Jurisdiction Index ("JI") published by Group Financial Crime to assess the jurisdictional risk of customers (e.g. for customer acceptance, associated person due diligence, etc.). Further details are available in the Group's Jurisdiction Index.

6 Procurement

This is the process by which the PIAS obtains goods or services from an external supplier. Procurement could be a high risk area for bribery and corruption, particularly if the supplier is acting on PIAS's behalf. The risks involved in the procurement of goods and services, where the supplier is not in a position to obtain or retain business advantages for PIAS, are more likely to relate to passive bribery. Whilst passive bribery does not expose PIAS to the risk of prosecution for the corporate offence of "failing to prevent bribery", it remains prudent to guard against this risk for sound commercial reasons. All procurement activities should be undertaken in accordance with the PIAS Procurement and Outsourcing manual.

Where the activity has been outsourced to a 3rd party provider, it is important that a higher standard of due diligence, governance and oversight apply to these relationships.

7 Transaction Monitoring

PIAS is responsible for monitoring transactions related to that market's activities on an ongoing basis to help identify unusual activity which may be connected to financial crime.

PIAS has a risk-based transaction monitoring framework that documents relevant financial crime scenarios, identifies transactions to be monitored and establishes the type and frequency of transaction monitoring required for each in accordance with guidance from Group Financial Crime.

Transaction monitoring should be performed in accordance with requirements determined by the relevant MAS Notice and other AML/CFT laws, regulations or applicable Notices, whether in Singapore or elsewhere as applicable.

The transaction monitoring framework and thresholds must be documented, approved by the Designated individual and PIAS Risk Committee and reviewed at least annually.

Transactions identified as unusual or potentially suspicious through transaction monitoring controls will be reviewed, investigated and concluded in a timely manner.

8 Risk Reporting

8.1 Code of Business Ethics Reporting

In order to help identify instances of potential bribery or corruption, PIAS uses the Gifts and Entertainment (G&E) Declaration form to administer the provision and receipt of gifts, entertainment, charitable or political contributions (generally political contributions are prohibited), Conflict of Interest (COI) Declaration form (Appendix 1) for any actual or perceived conflict of interest and is recorded in the COI register for review and approval.

An annual attestation on conflicts of interest is required by employees.

8.2 Gifts and Entertainment – General

Gifts

PIAS maintains the G&E Register to record both the offering and receipt of gifts and entertainment or hospitality. All gifts and entertainment which exceed the following minimum values must be recorded in the gift and entertainment register and reviewed by the Direct Line Manager. A copy of the register and line manager's approval should be sent to the Financial Crime team for review.

- gifts given or received and accepted or declined having a value more than SGD100 or
- entertainment offered or received and accepted or declined exceeding SGD150 per person per event
- entertainment / hospitality provided, offered or received and accepted or declined having a value more than SGD500 per person per event

Direct line managers may approve the offer and receipt of gifts and entertainment up to S$500. All gifts and entertainment that exceed S$500 will need to be approved by a member of the OpCo/the CEO of a subsidiary.

In Asian culture, it may be considered offensive to refuse a gift, especially during festive seasons. Employees may accept a token gift of no commercial value providing that it would not place the employee in a compromising position and if refusing the gift may jeopardize business relations.

All other prospective offers (whether to or by an employee) of gifts or entertainment falling outside the guidelines but which reflect customary and transparent business practice in a particular market must be referred to the employee's line manager and recorded in the Gifts and Entertainment Register.

All gifts with a value of SGD100 or more, given or received, must be declared in the Gifts and Entertainment form (Appendix 2) and approved by the employee's line manager whether they were accepted or declined. In addition, all gifts valued at more than $500, given or received, must be approved by PIAS CEO.

Cash gifts (such as red packets) of up to S$100 may be accepted or given only around the Chinese New Year period and at occasions like weddings and funerals. Cash gifts with a value exceeding S$100, accepted or given around the Chinese New Year period and at occasions like weddings and funerals must be declared in the Gifts and Entertainment Declaration Form (Appendix 2) and approved by the employee's line manager. There should be no cash gifts accepted or given outside of the festive Chinese New Year period and occasions like weddings and funerals. Line managers should exercise greater scrutiny for cash gifts.

In all cases, regardless of value, the Gift and/or Entertainment/Hospitality must be considered in light of all the given circumstances and must not be improper, excessively lavish or construed as a potential or actual bribe (i.e. intent to induce improper conduct).

When offering or accepting Gift and/or Entertainment/Hospitality, all employees must:

- ensure approval is sought in a timely manner
- for gifts and hospitality given by a PIAS employee, approval must be sought before an offer is made
- for hospitality given to a PIAS employee, approval must be sought before acceptance
- for gifts received by a PIAS employee, approval should be sought before acceptance where possible or failing that approval must be received within one week of receipt
- ensure appropriate approval is sought from local senior management and/or line manager
- ensure the gift and/or entertainment/hospitality is recorded within the register and is supported with sufficient details of:
    - the gift or hospitality being offered or received

- details of involved parties
- value of gift or hospitality
- approval audit trail (including where gifts and hospitality are declined)

Red flag indicators are used to identify abuse of the gifts and hospitality policy. Some red flag indicators may include:

- Repeat hospitality requests,
- Understating values to circumvent the gift and hospitality limits,
- Acceptance of goods (over nominal value) which is part of a cultural tradition (i.e. during a festive season) etc.

There are procedures in place for appropriate quality assurance (QA) and oversight of the gifts, entertainment and hospitality register.

PIAS has a zero tolerance for deliberate breaches of its gifts, entertainment and hospitality requirements. PIAS is committed to comply with the Group Standards on Conflicts of Interests, Gifts & Entertainment and Charitable Donations & Sponsorships and its relevant guidelines and procedures.

Entertainment

All Singlife Group employees must obtain their line manager's approval and record all entertainment offered or received exceeding the value of S$150 per person per event in the Gifts and Entertainment Declaration Form (Appendix 2), whether the event was accepted or declined. In addition, all entertainment valued at more than $500 per person per event, offered or received, must be approved by PIAS CEO.

8.3 Gifts and Hospitality Involving Public Officials

A public official is defined broadly as any current or former government officer, employee or other representative of any government, publicly funded organisation, government-owned or controlled entities, royal or governing family, or political party.

The provision of Gifts to public officials are prohibited.

If the entertainment / hospitality is being provided to a Public Official, extra care should be taken to avoid any suggestion that the hospitality is intended to influence the Public Official. Entertainment / hospitality must not be provided to Public Officials where it would be in breach of the policies or rules applicable to Public Officials.

PIAS requires employees to seek pre-approval from line managers for all entertainment/ hospitality offered to Public Officials (except for hospitality of low value, such as tea, coffee,

biscuits or sandwiches provided as a normal business courtesy) by recording such entertainment/ hospitality in the Gifts and Entertainment Register.

At a minimum, PIAS:

- identifies and documents which public officials are involved
- identifies and documents the purpose of the gift or hospitality
- seeks appropriate senior management approval before the offer of the gift or entertainment /hospitality occurs
- documents within the gifts and entertainment register including stating the fact that the individual is a public official

8.4 Charitable Donations and Sponsorships

Charitable donations and sponsorships can provide a means to pay a bribe to a third party and as a result, controls need to be in place to manage this risk.

Charitable donation or sponsorship is prohibited if it confers a personal benefit on a Public Official or if the donation is part of an exchange of favours with the Public Official.

Charitable Donations

Charitable donations should be construed in the widest possible terms and include the following:

• Corporate donations
• Corporate matching of employee giving
• Employee volunteering & non-monetary corporate donations (e.g. use of PIAS office space)

Charitable donations made in a personal capacity are unlikely to pose any risk to PIAS. However, if an employee has any reason to believe that a charitable donation or sponsorship made in a personal capacity creates the risk of bribery and corruption and/or reputational damage to PIAS this must be referred to the line manager or the Risk & Regulatory Team.

Sponsorships

Sponsorship agreements are when PIAS as the sponsor, contractually provides financing or other support in order to establish a positive association between PIAS' image, identity, brand, products or services, with a sponsored event, organisation, activity or an individual. Broadly defined, sponsorship is carried out to gain marketing and promotional benefits.

Due Diligence for Charitable Donations and Sponsorships

Before making a charitable donation or signing a sponsorship/partnership agreement, PIAS must conduct basic due diligence (Appendix 3) to ensure:

- the charity/third party is properly registered/identified
- the charity/third party is not on a relevant international or local sanctions list
- there are no current bribery and corruption or other criminal investigations, prosecutions or allegations in the public domain connected to the third party
- where there are PEPs, public officials, or other individuals with a close connection to the third party who are in a position, or may be in a position, to award contracts, or government authorisations/licences, the potential conflicts of interest are identified, risk assessed and appropriately managed as there is a high risk that this type of donations would be considered as a bribe or a facilitation payment and donations at the request of a public official are prohibited.
- there are no conflicts of interest that exist in relation to the person requesting the sponsorship/ donation, the charity/ third party or connected individuals
- there is no other evidence that the donation/sponsorships are or will be used as a bribe

All charitable donations and sponsorships are subjected to basic due diligence with the completion of the 'Donations and Sponsorships Due Diligence' form. Name-screening is done on the organisation and its key personnel. If any of the due diligence requirements on the formare not met, the request must be referred to the Risk & Regulatory Team so that it may be subjected to greater scrutiny.

For employee volunteering & non-monetary corporate donations, due diligence is only required when the cumulative value exceeds SGD10,000 (or equivalent) within a rolling 12-month period.

Approvals

All corporate sponsorships should be approved by the Group Head, Marketing. All charitable donations should be approved by the Group Head Marketing and the Group Head, People Function.

Frequency of Due Diligence

All due diligence reviews are valid for 12 months from the date of review unless there are significant changes to the key corporate personnel or the organisation's nature of business. Charitable donations and sponsorships that are over 12 months from the initial due diligence review date are subject to the full due diligence requirements outlined above.

Donations at the request of a public official are prohibited. There is a high risk that this type of donations would be considered as a bribe or a facilitation payment.

8.5 Social Benefit Projects or Charities

If PIAS is entering a new line of business or developing an existing one, and a requirement is imposed to enter a social benefit project or to donate to such a project or charity, approval should be obtained from Risk & Regulatory Team, who will need to examine whether such a donation could be considered a bribe.

PIAS ensures that there are procedures in place which require documented due diligence, a risk assessment and for the relevant approval of any such payment. This is to assess the viability of the charity or organisation and as part of our risk management approach.

PIAS ensures that there are procedures in place for appropriate quality assurance (QA) and oversight of charitable donations and sponsorships.

PIAS has zero tolerance for Charitable Donations/Contributions being made prior to the completion of Due Diligence and obtaining the relevant approval.

8.6 Political Contributions

Political contributions, made by or on behalf of PIAS (even if made by an individual), can often be viewed as inducements to public officials to retain or obtain business advantages and give rise to increased bribery and corruption risks. As a result, such contributions are generally prohibited by PIAS. In very limited circumstances, political contributions may be considered but must not be made before approval is obtained in line with Local and Group Legal, Company Secretarial and Public Policy standards.

Direct and indirect political contribution may include but are not limited to:

- donations to political parties and organisations
- payments to political candidates or members of governments and associated legislative office such as high-level civil servants

Political contributions can take the form of sponsorship and the provision of free or discounted services or facilities.

PIAS has procedures in place designed to prevent inappropriate or illegal political contributions being made on behalf of PIAS. Where such a request is made, full due diligence and risk assessment of the payment must be completed and must be fully documented with the relevant approval for the contribution being obtained and must be referred to the line manager or the Risk & Regulatory Team.

PIAS has zero tolerance for Political Donations/Contributions being made prior to the completion of Due Diligence and obtaining the relevant approval.

8.7 Conflicts of Interest

All new staff should declare any Conflicts of Interest when joining the company as part of the hiring process and all existing staff are required to declare any Conflicts of Interest on an annual basis as part of the annual mandatory training.

Conflicts of interests ['COIs'] occur when the personal or business interests of an employee or a party closely associated with the employee conflict with, or could reasonably be perceived to conflict with, the interests of PIAS.

An employee who is in a conflicted position may influence a business decision or outcome which may not be in the best interest of PIAS, our policyholders and shareholders. If that conflict is not identified, reported and managed to a position where the risk is mitigated, the relevant employees and PIAS could be exposed to legal and/or regulatory risk, or if in the case of a breach of the Singlife Group Business Ethics Code, subjected to disciplinary action.

This includes using the following for private gain by the employee, and/or any member of his/her family, friends or business associates:

a) An employee's work position
b) Confidential business information
c) Corporate time, materials, property and/ or facilities
d) Insider dealing
e) External business activities, or taking on additional employment

Examples include but are not limited to:

- a family member, close relative or friend of an employee works at a company that has close connections to PIAS e.g. a preferred supplier
- a family member, close relative or friend of an employee works at another company that provides similar services to PIAS and can expose PIAS to increased risks e.g. a claims management company
- where an employee is line managed or works closely with a family member, close relative, friend or someone with whom they are in a relationship with
- where an employee has an external business interest, shareholding or appointment
- where an employee takes on additional employment including contract, freelance and consultancy work
- where an employee takes on an internal position such as a board directorship in a related company which may also give rise to a potential, perceived or actual conflicts of interests
- where PIAS provides loans, infrastructure or other resources to a third-party with which it does business (e.g. where PIAS funds the set-up of an insurance broker that may then be expected to promote the company products)

The purpose of the Conflicts of Interests (COI) Form (Appendix 1) is to highlight and record any instance where an employee has or is perceived to have external business interest in an organisation (an "External Party") with which PIAS has or may be about to enter a commercial relationship in circumstances which may prejudice PIAS relationship with that External Party or any other third party or may give rise to potential, perceived or actual conflicts of interests.

Examples of external business activities which should be declared are contract/ freelance/ consultancy work, external business, second employment, shareholding, political position and directorships.

Category	Definition
Potential	Circumstances which may lead to or develop into an actual conflict of interest
Perceived	Even where there is no evidence of improper actions, a day-to-day situation can create the appearance of impropriety, which could undermine confidence in the ability of Singlife or its employees to act properly and fairly.
Actual	A conflict of interest which presently exists

In certain circumstances, an internal position such as subsidiary board directorship, activity or relationship might create conflicts of interests. This could be because of an internal business arrangement or a personal relationship which may also give rise to a potential, perceived or actual conflicts of interests.

PIAS must at a minimum, ensure that:

- employees are aware of the need to avoid conflicts of interest and to seek approval for any action which they believe could potentially give rise to a conflict of interest
- a conflict of interest form is in place and maintained to enable employees to formally record potential or actual conflicts of interest to the attention of the board and senior management
- All new staff are to declare any Conflicts of Interest when joining the company as part of the hiring process and all existing staff are required to declare any Conflicts of Interest on an annual basis as part of the annual mandatory training
- conflicts are appropriately approved by line manager and remedial action should be taken to resolve the potential conflict

Any potential Conflicts of Interest arising from External Business Activities or Internal Activities/ Relationships should be declared in the Conflicts of Interest form and approval obtained from the line manager.

Procedures:

- For ad-hoc Conflicts of Interest declarations, the Conflict of Interest Declaration Form should be completed by PIAS staff (including contract staff) if/when there is any perceived or actual conflict of interest (refer to appendices page on Darwinbox Process Flow for COI/G&E Declaration) on the submission and approval process.
- The Declaration Form via Darwinbox will be sent to the employee's line manager for approval and the Risk & Regulatory Team will receive a notification for review.
- Each potential conflict is to be approved by the line manager and remedial action should be taken to resolve the potential conflict.

8.8 Facilitation Payments

Facilitation payments involve an illegal or unofficial payment made in return for services which the payer is legally entitled to receive without making such a payment. It is normally a relatively minor payment made to a public official or person with a certifying function in order to secure or expedite the performance of a routine or necessary action, such as the issue of a visa, work permit or customs clearance.

Facilitation payments may also be requested to secure access to distribution channels for PIAS products and services which would otherwise not be available to Singlife.

Facilitation payments or inducements to or from public officials are prohibited. PIAS has no appetite for acts of bribery or corruption by an employee or person associated to the Company.

9 Suspicious Transactions or Unusual Activity Reporting

9.1 Reporting of Bribery and Corruption Related Cases

This section relates to any incident of potential bribery or relevant local legislation, with direct or indirect linkage to PIAS, including its employees, agents, suppliers, business partners, directors, intermediaries, etc. It does not include suspected bribery or corruption unrelated to PIAS. For example:

- customer X offers PIAS employee a bribe – covered in this section
- customer X pays company Y a bribe – not covered by this section (although there may be a separate reporting requirement, for example under AML legislation)
- company X uses Singlife product to bribe company Y – covered by this section.

PIAS educates employees regularly where a potential incident of bribery or corruption has been identified it must be referred to Group Internal Audit, using 'Speak Out Charter' or following the

local reporting procedures. This includes requests for a bribe, such as facilitation payments, even if the request is refused.

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

As part of any investigation (whether conducted by Group Internal Audit or not) a root cause analysis of the incident will be undertaken to determine any lessons to be learnt and whether any changes to systems, controls, policies and procedures are required to reduce the likelihood of such an incident reoccurring. This must include re-visiting the bribery and corruption risk assessment and undertaking deep dives into specific aspects of the incident such as the associated person due diligence.

The following bribery and corruption incidents must be reported to the Group Head of Legal and Compliance:

- all actual incidents of bribery or corruption (those that are proven, substantiated or otherwise believed to be factual)
- all requests for a bribe (including facilitation payments) whether refused or not

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 has suspicion that a transaction may be connected with bribery and corruption, he shall immediately refer the matter to PIAS' Designated Individual who is PIAS' Head of Risk & Compliance. Alternatively, he can send an email to the Risk & Regulatory Team at pias.compliance@singlife.com.

All relevant cases will be reported to the Corrupt Practices Investigation Bureau ("CPIB") online. Website: https://www.cpib.gov.sg/e-complaint – done by ABC Reporting Officer or delegate.

All allegations/incidents are also included in the Management Information ("MI") sessions. This includes local management committee and PIAS Risk Committee.

9.2 Reporting of Suspicious or Unusual Activity

All employees and representatives shall keep in mind of their obligations to report suspicious transactions as required by section 39(1) of the Corruption, Drug Trafficking and Other Serious

Crimes (Confiscation of Benefits) Act 1992 (“CDSA”), and the Terrorism (Suppression of Financing) Act 2002 (“TSOFA”). The TSOFA not only criminalises terrorism financing, it also imposes a duty on everyone to provide information pertaining to the terrorism financing to the police.

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 has suspicion that a transaction may be connected with money laundering or terrorism financing, bribery & corruption, fraud or tax evasion, he shall immediately refer the matter to PIAS’ Designated individual who is PIAS’ Head of Risk & Compliance. Alternatively, he can send an email to the Risk & Regulatory Team at pias.compliance@singlife.com

The Risk & Regulatory Team shall evaluate and document the basis of their determination in the Suspicious Transactions Register whether a matter should be referred to STRO within 15 business days, unless the circumstances are exceptional or extraordinary. Any exception (i.e. exceed 15 business days) shall be explained and documented in the Suspicious Transactions Register. The Head of Risk Management & Compliance will review the report before it is submitted to Singapore Police Force via STRO Online Notices and Reporting Platform (SONAR).

10 Incident Reporting (Internal Audit)

In order for Internal Audit to investigate incidents in an effective and timely manner, PIAS reports using any available channel (e.g. direct to Internal Audit or using Speak Out (by email, telephone or mobile application)), suspicions or alleged instances of internal and non-customer malpractice or financial crime, including possible breaches of the Business Ethics Code.

In order to achieve this, PIAS reports such incidents to Internal Audit within 2 business days.

11 ‘Speak Out Charter’

“Speak Out Charter” is a confidential reporting process to enable employees, contractors, outsource providers and other third parties to report behaviour in the workplace (by Singlife or Third Parties) that may be a breach of Singlife Business Ethics Code; may be illegal, criminal, or unethical; or may be an abuse of our systems, abuse of any processes or policies.

“Speak Out Charter” provides a confidential, reliable, credible and secure reporting mechanism. PIAS sends active reminders to all management and staff of this service, including ensuring that management and staff understand their obligation to report in accordance with Group’s Business Ethics Code.

12 Compliance Monitoring

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

The scope, nature and frequency of monitoring will be documented as part of the Financial Crime Work Plan, considering any local regulatory requirements for regular independent assurance. At minimum, compliance testing will include the following key risk areas for Financial Crime:

- Financial Crime training and awareness
- Financial Crime responsibility/ownership
- Financial Crime risk assessment – market risk assessment and product/services risk assessments
- Management information (including completeness, accuracy and analysis)
- Governance, reporting (both internal and external) and escalation
- Review of associated person due diligence (including employees)
- Procurement activities
- Adequacy of red flags and other detection systems
- Responding to law enforcement and incidents
- Governance, reporting and escalation
- Investigation procedures
- Financial Crime record keeping

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 & Compliance [“RM&C”], and PIAS Risk Committee.

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

13 Training

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

Where additional training is required for department at high risk of financial crime, tailored training will be provided.

On an annual basis, Financial Crime training materials are reviewed and update to reflect any local regulatory/legislative or market changes.

The Risk and Regulatory team (with the support of People Function) will monitor the completion of AML/CFT training within the stipulated timeline. The Risk and Regulatory team will take appropriate action against those who are unable to complete the AML/CFT training without a reasonable cause.

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 Group Financial Crime Team monthly, using the Group Financial Crime MI pack conforming to the format, template and requirements set by the Group Financial Crime Team.

15 Board and Management Reporting

The Risk and Regulatory team prepare and present a quarterly financial crime report to the business entity's Operational Risk Committee and to the Board Risk Committee. The report must provide information on the financial crime risk profile of the company, performance against each of the 6 Group Financial Crime preference statements, the effectiveness of risk mitigating controls and any material matters such as regulatory violation together with the remediation actions.

16 Record Keeping

Record Retention and Retrieval

PIAS has implemented procedures, systems and controls to enable relevant financial crime records to be retained, retrieved and if necessary, deleted to comply with local legislation and Group's Financial Crime Policy/ 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, ECDD 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.

Appendices

Appendix 1 -Conflict of Interests Declaration Form

Appendix 1 –
Conflict of Interests

Appendix 2 - Gifts & Entertainment Declaration Form

Appendix 2 - Gifts
& Entertainment De

Appendix 3 - Charitable Donations and Sponsorships Due Diligence Form

Appendix 3 -
Charitable Donation

Darwinbox Process Flow for COI/G&E Declaration

DarwinboxProcess
Flow for COI G&E D