Financial Crime Risk Management Policy [FCRMP]

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
18/8/2020	2	• Elaboration on Compliance Testing – Section 10 • Update on review of Financial Crime training material – Section 12 • Inclusion of Access to Customers' Personal Data	Kenneth Goh	PIAS Risk Committee
01/09/2022	3	• Annual Review of Policy	Kelly Lam/ Tang Ming Yang/ Maisuri Abdul Karim	PIAS Risk Committee
10/11/2023	4	Section 3.2 "Identifying, Assessing and Understanding Financial Crime Risks" • Added external TF risk environment, TF risk exposure, potential financing of other existing or new terrorist groups and new and emerging international typologies in which TF can be financed Section 8.2 "Suspicious Transactions or Unusual Activity Reporting" • Added to share additional information or useful insights with Law Enforcement Agencies through the filing of supplementary STRs. Section 8.3 "Suspicious Transactions or Unusual Activity Reporting – External" • Added to share additional information or useful insights with Law Enforcement Agencies through the filing of supplementary STRs. • Annual Review of Policy	Mei Na Chua / Maisuri Abdul Karim / Tang Ming Yang	PIAS Risk Committee
30/11/2024	5	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 all applicable regulations that may be issued by the relevant authorities in Singapore. The applicable local regulations for Financial Crime Management Policy ("Policy") are set out in Financial Advisers Act 2001 ("FAA"), Financial Advisers Regulations ("FAR") and its ensuing Notices/Guidelines.

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

Targeted financial sanctions are governed by the financial sanctions issued by Monetary Authority of Singapore ("MAS").

Anti-bribery & corruption ["ABC"] is locally governed by Prevention of Corruption Act 1960 ("PCA") and Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA").

Fraud is locally governed by the Financial Advisers Act 2001 ("FAA"), MAS FAA Notice 17 – Notice on Reporting of Suspicious Activities & Incidents of Fraud ("FAA-N17") and LIA MU 55/19 – Life Insurance Association guidelines on risk management practices in respect of life insurance intermediary fraud risk.

The use of data is governed by Data Governance and Data Privacy Business Standards. The local applicable legislation is the Personal Data Protection Act 2012 ("PDPA").

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.

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:

1) **Breaches of law, regulation and policy relating to financial crime**
   PIAS has no appetite for intentional or repeated breaches of law, regulation or policy related to financial crime. Recognising that financial crime risk events of this nature will occur, PIAS will, to limited degree, tolerate accidental breaches.

2) **High Risk Countries**
   As a general principle, PIAS has no appetite for conducting business involving, customers and counterparties based in or from very high risk countries without an appropriate approval.

   PIAS has limited appetite for conducting business involving customers and counterparties based in or from high risk rated countries.

3) **Facilitation of Tax Evasion**
   PIAS has no appetite for acts of intentional facilitation of tax evasion by employees, Financial Adviser Representatives or other persons associated to the Group. PIAS seeks a continually improving trend in managing this risk and ensures any accidental or intentional risk events of this type are reported and investigate.

4) **Bribery and Corruption**
   PIAS has no appetite for acts of bribery or corruption by an employee or person associated to 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 the payment of inducements to public officials

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

5) Anti-Money Laundering

i. PIAS has no appetite for intentionally accepting assets suspected to be of criminal origin without lawful authority to do so.
ii. PIAS has no appetite for conducting business with prohibited customer or segment types.
iii. PIAS has no appetite for conducting business with restricted customer or segment types.

6) Fraud

I. PIAS has no appetite for acts of fraud or dishonesty perpetrated by employees, directors or Financial Adviser Representatives.
II. PIAS has no appetite for acts of fraud or dishonesty directed against or enabled through PIAS by customers, suppliers, distributors and third parties including those where PIAS has no business relationship.
III. PIAS seek 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 Enterprise Wide Risk Assessment (EWRA) or occurrence of risk events), PIAS will consider issuing additional internal communications as part of an ongoing training and awareness programme in order to raise awareness of PIAS approach to financial crime risks and the consequences of non-compliance.

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.

PIAS will encourage all suppliers to sign up to Singlife Supplier Code of Behaviour, where the suppliers commit 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 to 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 by PIAS 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 on PIAS's 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, the PIAS Risk Committee will review and approve any financial crime policies and procedures as well as approve the approach in PIAS 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
- Execute the requirements of an adequate and appropriate Financial Crime Risk Management Framework

- Escalations to Risk & Regulatory Team (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 Second line of defence ("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 Strategy

- 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

Advisory and Oversight

- 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 MI 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

Policy

- 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 which ensure compliance with applicable regulatory requirements, Singlife Group Financial Crime Policy and all applicable policies, standards and guidance.

Financial Crime Prevention Programme

- Financial Crime Business Standard Attestation for PIAS (in MetricStream or equivalent)
- Quarterly review of PIAS' Gifts and Hospitality Register and Conflicts of Interest entries
- Bribery and Corruption Detection Checks – Review of Gifts and Hospitality expenses (including sponsorships and donations) in Finance
- Annual reminder to all employees on registering Gifts & Hospitality 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 to Group Financial Crime 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 for Global Name Screening for all categories (i.e. sanctions, Politically Exposed Persons) and High Risk Countries 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 GNS, Fraud and Suspicious Transactions Reporting MI review
- Attend to Law Enforcement enquiries, where required

2.5 Review of Financial Crime Programme

PIAS will review its Financial Crime Programme on a regular basis (at least annually), to ensure they are fit for purpose and reflect any changes to its 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 Appointment of a Money Laundering Reporting Officer ("MLRO")

PIAS Chief Executive Officer (CEO) will identify and appoint a member of Senior Management as the PIAS' Designated Individual, who will be the PIAS Money Laundering Reporting Officer ("MLRO") and ultimately accountable for financial crime risk management in PIAS.

Where appropriate, PIAS may appoint additional Designated Individuals at business or cell level, provided that it is clear who has ultimate accountability for financial crime. All appointments will be approved by PIAS Risk Committee.

The appointed person will understand to which they have been appointed and how the financial crime legal, regulatory and internal policy requirements will apply. The Designated Individual will understand the level of financial crime risk exposure in PIAS. With an appropriate level of seniority, skills, knowledge and experience in implementing, maintaining and monitoring compliance with financial crime standards, the Designated Individual will have sufficient standing to act independently under his/her own authority.

All appointments (including delegations) will be fully documented including details of accountabilities and responsibilities and will be agreed on at least an annual basis by Senior Management.

PIAS CEO shall ensure that the role of Designated Individual is covered at all times. Any gaps in coverage of over 1 month will be reported to PIAS Risk Committee and Group Head of Legal & Compliance, together with a plan for resolution.

For PIAS, the Designated Individual is the Head of Risk Management & Compliance.

2.7 Responsibilities of MLRO

The key responsibilities of the MLRO include:

a) promoting compliance with applicable regulations:
   - MAS Regulations
   - the relevant MAS Notices, Directives and Guidelines; and
   - laws, regulations, notices applicable to any overseas subsidiary;

b) taking overall charge of all AML/CFT matters, including MLRO responsibilities;

c) communicating regulatory changes and development to management, employees and financial adviser representatives, where relevant;

d) investigating and ensuring appropriate remediation actions are taken for any actual or suspected ML/TF issues;

e) reporting, or overseeing the reporting of suspicious transactions;

f) advising and training of financial adviser representatives, employees and officers on developing and implementing internal policies, procedures and controls on AML/CFT;

g) reporting to senior management on the outcome of any reviews conducted on compliance with any AML/CFT regulatory requirements;

h) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews to the senior management and board of directors; and

i) conducting an enterprise wide risk assessment to identify and assess ML/TF risks on an enterprise-wide level, at least once every 2 years or upon a material trigger event (change in risk profile).

MLRO may delegate activities to other individuals provided such alternatives are competent to fulfil the required activities and will ensure that there are appropriate oversight controls in place. The MLRO will remain accountable for all activities that are delegated.

To enable unbiased judgments and facilitate impartial advice to management, the MLRO will be appointed from the second line function. Where any conflicts between business lines and the responsibilities of the MLRO arise, the matter must be escalated to the Group Head of Legal & Compliance who will ensure that the AML/CFT concerns are objectively considered and addressed.

2.8 Appointment of a Nominated Officer

PIAS CEO will identify and appoint a Nominated Officer who is responsible for reviewing internal suspicious activity reports relating to Money Laundering and Terrorist Financing and where necessary reporting externally to local authorities.

The appointed person should have an appropriate level of seniority, skills, knowledge and experience in reviewing and investigating actual, potential or suspect acts of money laundering and continue to maintain adequate knowledge throughout the course of their appointment.

The Nominated Officer should have sufficient standing to act independently under his/her own authority and can decide independently if a suspicious activity report (SAR) needs to be made to the relevant authorities. The Nominated Officer ought to be sufficiently independent to avoid any potential conflict of interest, arising from the business' commercial interest. The nominated officer is required to understand the company /business to which they have been appointed and how the financial crime legal, regulatory, internal policy requirements and external reporting requirements apply.

The appointment of a nominated officer, including any delegates, are fully documented including details of accountabilities and responsibilities. PIAS' Nominated Officer is the Team Lead of the

Risk & Regulatory Team who reports to the Head of Risk Management & Compliance. All nominated officer appointments are agreed by PIAS Risk Committee.

The appointment of a Nominated Officer under Singapore Legislation is not subjected to regulatory approval. The MLRO will make sure that the role of the nominated officer is covered at all times. In order to cover gaps in coverage (i.e. due to annual leave, etc.) the role may be temporarily delegated provided it is appropriately approved, documented and communicated to relevant employees. Whilst the activity can be delegated, the ultimate responsibility remains with the nominated officer.

The legal/regulatory responsibilities of the Nominated Officer should be documented within their role profile or job description.

2.9 Responsibilities of Nominated Officer

The responsibilities of the Nominated Officer include receiving and reviewing internal reports relating to actual, potential or suspected acts of money laundering and/or terrorist financing.

The Nominated Officer is the primary interface (in relation to AML/CFT activity) to Law Enforcement Agencies, including responding to court orders and other official requests received relating to AML/CFT investigations. The Nominated Officer ensures that there are appropriate processes in place to monitor and manage the receipt, investigation and disclosure of SARs.

Where any of the responsibilities for undertaking investigation of internal reports and any subsequent disclosure to Authorities is delegated, the Nominated Officer and MLRO will approve the competence of any alternates and ensure there are appropriate oversight controls in place.

2.10 Notification of Appointments

PIAS provides to Group Financial Crime, details of the individuals appointed as its Designated Individual, MLROs and Nominated Officer.

Details 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.

2.11 Appointment of Designated Individual

PIAS CEO will identify and appoint a member of senior management as the designated individual, who is ultimately accountable for financial crime risk management in PIAS.

Where appropriate, PIAS may appoint additional designated individuals at business or cell level, provided that it is clear who has ultimate accountability for financial crime. All appointments are approved by the PIAS Risk Committee.

The appointed person ought to understand the company to which they have been appointed and how the financial crime legal, regulatory and internal policy requirements apply. The designated individual understands the level of financial crime risk exposure within their market/business/cell. With an appropriate level of seniority, skills, knowledge and experience in implementing, maintaining and monitoring compliance with financial crime standards, the designated individual also has sufficient standing to act independently under his/her own authority.

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

PIAS CEO will make sure that the role of designated individual is covered at all times. Any gaps in coverage of over 1 month are reported to PIAS Risk Committee and Group Financial Crime, together with a plan for resolution. For PIAS, the designated individual is the Head of Risk Management & Compliance.

Where any conflicts and the responsibilities of the AML/CFT Compliance Officer arise, the matter must be escalated to the Group Head of Legal & Compliance who will ensure that the AML/CFT concerns are objectively considered and addressed.

2.12 Responsibilities of Designated Individual

The responsibilities of the Designated Individual for financial crime risk management include any local regulatory or legal accountabilities for financial, active involvement in financial crime risk management, supervision and critical decision-making processes as well as oversight and input into the design and ongoing review of local financial crime policies, procedures, systems and controls.

Being a key member of financial crime governance forums/committees, the Designated Individual provides oversight of and involvement in PIAS financial crime risk assessment(s) and reporting process, ensuring adequate financial crime resources are deployed to mitigate identified risks.

The Designated Individual demonstrates ‘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 Group as well as assessing and reporting on the adequacy of the financial crime programme through ongoing testing, management information and board/committee reporting.

This ensures the PIAS Risk Committee and the Board are adequately informed of internal and external financial crime developments and oversight of financial crime related breaches and the provision of feedback to board on levels of compliance are provided.

The Designated Individual may delegate activities to other competent persons. However, the ultimate responsibility for the management of financial crime risk remains with the Designated Individual.

The responsibilities of the Designated Individual are documented within their role profile or job description.

2.13 Designated Individual - Review Process

The on-going appropriateness of the Designated Individual for financial crime risk is assessed on a regular basis to ensure they remain appropriate for the role. This includes assessment through the annual performance management process (including any ad hoc performance issues) and consideration of suitability against the wider team's seniority, skills, knowledge and experience.

The evidence of continued senior management financial crime training and/or attendance at relevant financial crime events are required.

3 Risk Assessment

3.1 Enterprise-Wide Risk Assessment

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.

In reviewing its risk-mitigating controls for adequacy, the following should be considered:

a) the inputs from country's financial intelligence unit (the STRO, in the case of Singapore);

b) any new or emerging trends in terms of customer profiles or arising from products and services or channels of distribution, which were not previously observed;

c) any new regulatory developments;

d) any audit or regulatory observations;

e) any feedback from the business and senior management; and

f) any material ML/TF trends in the public domain.

3.2 Identifying, Assessing and Understanding Financial Crime Risks

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

- the customers;
- the countries or jurisdictions where the customers are from or in;

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

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

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

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

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

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

3.3 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.

3.4 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 is 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.

3.5 Risk-Based Controls

The Head of Risk Management & Compliance will use Enterprise-wide Risk Assessment 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 is documented (either as a stand-alone document or incorporated in other relevant documents) and takes into account of Financial Crime Policy.

This approach is 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
- the payee (where the payee is not the customer)

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

- full name, including any aliases;
- unique identification number (such as an identity card, passport or birth certificate number) or where the customer is not a natural person, the incorporation number or business registration number);
- residential address or where the customer is not a natural person, the incorporation number or business registration number);
- date of birth or where the customer is not a natural person, the incorporation number or business registration number); and
- nationality or where the customer is not a natural person, the incorporation number or business registration number)

We must verify the identities of customers using reliable and independent source data, documents or information in the form of:

a) NRIC, Birth Certificate, Passport or MyInfo (for a natural person) and
b) Certificate of incorporation or registration, deeds, partnership agreement or other reliable independent source documents (for a legal person or legal arrangement)

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.

It should be noted that the Group may collect, use and disclose the personal data of individual customers of any subsidiary entities within the group, including the personal data of any individual appointed to act on behalf of a customer, or an individual connected party of a customer, an individual beneficial owner of a customer, or an individual payee of any group business, without the respective individual's consent.

4.1.1 Beneficial Owners

In respect of private individuals, the customer is the beneficial owner, unless there are features of the relationship, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement to make proactive searches for beneficial owners where the customer is an individual. However, businesses must make appropriate enquiries where it appears that the customer is not acting on its own behalf.

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

In respect of a trust or similar arrangement, the beneficial owners include the settlor, the trustees, the beneficiaries and any individual who controls the trust.

4.1.2 Beneficial owners must be identified, and reasonable measures must be taken to verify their identities through the collection of relevant information.

PIAS shall not be required to inquire if there exists any beneficial owner in relation to a customer or a beneficiary that is:

a) an entity listed and traded on the Singapore Exchange;
b) an entity listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements and requirements relating to adequate transparency in respect of its beneficial owners;
c) a financial institution set out in Appendix 1 of FAA N06;
d) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or
e) an investment vehicle where the managers are financial institutions set out in Appendix 1 of FAA N06; or incorporated or established outside Singapore but are subject to and

supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless PIAS has doubts about the veracity of the CDD information, or suspects that the customer, beneficiary, business relations with, or transaction undertaken in the course of business relations for, the customer, may be connected with money laundering or terrorism financing.

4.1.3 Natural Persons Appointed to Act

We must also identify and verify the identities of natural persons appointed to act on a customer's behalf and verify the due authority of each natural person appointed to act by:

a) obtaining the appropriate documentary evidence authorising the appointment of such natural person by the customer to act on the customer's behalf; and

b) verifying that such natural person is the person authorised to act on the customer's behalf, through obtaining the person's specimen signature or other electronic means of verification.

4.1.4 Connected Parties

Where the customer is a legal person or legal arrangement, we must identify the connected parties of the customer, by obtaining at least the following information of each connected party:

a) full name, including any aliases; and

b) unique identification number (such as an identity card number, birth certificate number or passport number of the connected party).

However, where the ML/TF risks in relation to the customer are not high, and we are not able to obtain the unique identification number of the connected party after taking reasonable measures, we may obtain the date of birth and nationality of the connected party, in lieu of the unique identification number.

We must not issue insurance policies in fictitious names or where customer due diligence measures cannot be performed.

4.1.5 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.

4.1.6 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.

We must perform Customer Due Diligence when:

- we establish business relations with any customer;
- there is a suspicion of money laundering or terrorism financing; or
- we have doubts about the veracity or adequacy of any information previously obtained.

Therefore, CDD measures are conducted:

- at the application stage by financial adviser representatives, financial advisers (including banks) or by the customer himself on the company's insurance application portal; and
- when customers approach our Customer Service counter to carry out transactions.

If there are any reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct, or are property related to the facilitation or carrying out of any terrorism financing, the Group shall not establish business relations with the customer. An STR shall also be filed.

4.1.7 CDD Measures for Non-Face to Face Sales

Where there is no face-to-face contact, the Group shall perform CDD measures that are at least as robust as those that would be required to be performed if there was face-to-face contact.

These measures include obtaining a second identity document and performing customer call-backs.

4.1.8 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.

4.1.9 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 are risk-based to reflect the level of financial crime risk. This will take into account the role the associated person is undertaking for Singlife and the jurisdiction involved.
- the nature, extent and format of DD are 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 are documented in the business's FCRMP.
- DD will initially be completed at the commencement of a relationship and are kept up to date throughout the relationship according to a schedule determined in the business's FCRMP.
- DD evidence are retained and are retrievable.
- the quality, completeness and accuracy of DD are subject to a quality control process, and the nature, frequency and scope of this control process are documented in the FCRMP.
- the results of DD quality testing will form part of the business's Compliance monitoring and reporting.

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 Singlife's 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 is escalated to the 2nd line of defence, the Risk & Regulatory Team.

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

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 needs to identify 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 check, 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 will ensure that all employees attest annually to Group's Code of Business Ethics.

Due Diligence on Intermediaries

PIAS determines the additional due diligence activities required, where an intermediary wants to partner with PIAS. This due diligence is 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
- name screening of the firm and its directors

Where local legislation permits, PIAS may 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.

Reliance on Third Parties

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 remain with PIAS.

5 Name Screening (Sanctions and Higher Risk Persons)

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

Name screening may also uncover any person identified as being a Politically Exposed Person (PEP), a person from a higher risk jurisdiction and/or a person with adverse news relating to ML/TF or other financial crime. In such scenarios, the business must assess the risk of entering or continuing business relationship with the identified individuals or entities and obtain senior management approved as appropriate.

The screening against GNS is performed daily. Watchlists are maintained and reviewed by Dow Jones. The MAS Alert and Control List is maintained as a Private List and Group Financial Crime Compliance function will update the Private List as and when there are updates from MAS and upload it to GNS.

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 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 and set the approval mechanism (e.g. for customer acceptance, associated person due diligence, etc.). Further details are available in the Group's Jurisdiction Index.

6 Record Keeping

Record Retention and Retrieval

PIAS will implement procedures, systems and controls to enable relevant financial crime records to be retained, retrieved and if necessary, deleted to comply with local legislation and 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 ("STRO"), 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.

7 Ongoing Transaction Monitoring

PIAS is responsible for monitoring transactions on an ongoing basis to help identify unusual activity which may be connected to 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.

PIAS establishes 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. As far as possible, PIAS is to leverage on advanced

technologies such as artificial intelligence and machine learning capability to enhance the effectiveness of the monitoring.

The transaction monitoring framework and thresholds must be documented and approved by the Group Head of Legal & Compliance or if designated the Group Head of Financial Crime and endorsed by the relevant local governance committee for financial crime matters. The framework and threshold should be reviewed at least once every two years.

Transactions detected as unusual or potentially suspicious through the transaction monitoring controls must 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 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.

8.1.2 Gifts and Entertainment

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 and 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 recorded in the 'Gifts and Entertainment form' 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 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 Gifts 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 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:
    - Gift or Hospitality being offered or received
    - details of involved parties
    - value of Gift or Hospitality
    - approval audit trails (including where gifts and hospitality are declined)

PIAS has appropriate controls (including MI) in place to identify abuse of the Gifts and Entertainment policy. Some red flag indicators may include repeat hospitality requests, understating values to circumvent the gift and entertainment/hospitality limits, acceptance of goods (over nominal value) which is part of a cultural tradition (i.e. during a festive season) etc.

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 , 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.

8.1.3 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

8.1.4 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 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 form are 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.

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 as 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.

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.

Conflicts of Interests ["COIs"]

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 the company funds the setup of an insurance broker that may then be expected to promote the company products)

The purpose of the Conflicts of Interests (COI) Form 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.
- The Declaration Form should be sent to the employee's line manager for approval and the Risk & Regulatory Team for review.
- Each potential conflict is to be approved by the line manager and remedial action should be taken to resolve the potential conflict.

Facilitation of 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 PIAS.

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.

8.2 Reporting of Suspicious Transactions or Unusual Activity

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

PIAS keeps in mind the provisions in the CDSA and the TSOFA which provide for the reporting to the authorities, transactions suspected of being connected with ML/TF and implement appropriate internal policies, procedures and controls to meet the obligations under the law.

A transaction is deemed suspicious when it is inconsistent with the customer's known legitimate business or personal activities. PIAS considers the circumstances relating to the transactions in totality particularly where it appears unusual or does not make economic sense. Suspicious activity may occur at the onset of the business relation or after the business relation has been initiated. PIAS also considers cases where they were unable to complete the CDD, simplified CDD or enhanced CDD measures, and where the customer concerned is reluctant, unable or unwilling to provide any information requested by PIAS and subsequently decides to withdraw a pending transaction or account application or terminate an existing business relationship.

Employees are trained during induction, as well as periodic email reminders, on 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).

Records of all transactions referred to STRO, together with all internal findings and analysis done are properly kept by Risk & Regulatory Team or MLRO.

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

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

AML/CFT

All PIAS 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 Section 8 of 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 terrorism financing to the police.

If an employee or representative has suspicion that a transaction may be connected with ML/TF, he shall immediately refer the matter to the company's AML/CFT Compliance Officer (or MLRO). Records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them must be properly kept by the AML/CFT Compliance Officer.

Risk & Regulatory Team evaluates and documents the basis of determination in the Suspicious Transactions Register whether a matter should be referred to Suspicious Transaction Reporting

Office (“STRO”) within 15 business days and extend a copy to the Authority for information, unless the circumstances are exceptional or extraordinary. Any exception (i.e., reporting exceeds 15 business days) shall be explained and documented.

Customers with STRs filed shall be tagged in the system as high-risk customers that will be subject to ECDD (at the next trigger event) and enhanced ongoing monitoring, so as to mitigate the risk of PIAS being used for money laundering or terrorism financing activities.

Risk & Regulatory Team will also obtain regular updates from the STRO on their review of the Suspicious Transactions Reports filed by the Group.

Under Section 45 of the CDSA, the consequences for not reporting suspicious transactions to STRO are:

- for an individual, a fine not exceeding S$250,000, or imprisonment not exceeding 3 years, or both; and
- for a non-individual, a fine not exceeding S$500,000

Bribery or Corruption

This section relates to any incidents of potential bribery or corruption under 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.

Bribery involves the offer, promise, payment, transfer, request, or receipt of anything of value, to induce someone to perform their role improperly. Offering or accepting a bribe is a criminal offence. Paying or offering a bribe while acting on behalf of PIAS can also expose the company to criminal action.

What is expected from us?

- We reject the offer or payment of a bribe in any part of our business activity, anywhere in the world.
- We refuse to pay or offer a bribe, no matter how small, anywhere in the world.
- We complete relevant training to be able to identify and manage the bribery risks that may arise in our roles.
- We report all offers of a bribe, requests for a bribe or suspected corruption immediately to the Risk & Regulatory Team or MLRO.

As part of any investigation, a root cause analysis of the incident is 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.

Internal and External Fraud

This section relates to any incident of potential internal and external fraud under relevant local legislation, with direct or indirect links to PIAS, including its employees, agents, suppliers, business partners, intermediaries, etc. It does not include suspected internal and external fraud unrelated to PIAS.

There are 3 broad categories of insurance fraud, namely: (1) Policyholder and claims fraud; (2) Intermediary fraud; and (3) Internal fraud.

PIAS includes measures to identify and mitigate the risk of fraud, as well as the measures to monitor and detect any instance or suspicion of fraud. Examples of common red flags are if the policyholder has been declined coverage by other insurers due to non-disclosure; unusual product-client combinations; claimant provides inconsistent statements or information.

To mitigate the risk of intermediary fraud, PIAS must conduct appropriate due diligence and fit and proper assessment on the intermediary before establishing business relationship with the partner/agent. There should also be ongoing monitoring of the intermediaries' market conduct practices and sales performance and trends.

The business unit in PIAS who is responsible for the relationship should be vigilant of any unusual performance patterns and take action to understand the reasons for the exceptions. As a general policy, intermediaries must not be allowed to collect premium payments in cash.

To mitigate the risk of internal fraud, PIAS must ensure that proper segregation of duties, effective supervision and appropriate checks and balance controls (such as reconciliation of money received /paid) are in place and properly enforced.

PIAS undertakes a root cause analysis of internal and external fraud incidents to identify weaknesses in controls, such as training, red flags, data analytics, investigation methods, etc. Policies, procedures and training are also updated to reflect these control changes.

Tax Evasion

This section relates to any incident of potential facilitation of tax evasion under relevant local legislation, with direct or indirect links to PIAS, including its employees, agents, suppliers, business partners, directors, intermediaries, etc.

Tax evasion is the illegal non-payment or under-payment by a taxpayer of taxes due to the relevant authorities.

What is expected from us?

- We strictly prohibit any person associated with PIAS from doing anything that supports, encourages or facilitates tax evasion.

- We act with honesty and integrity and report any suspicion of tax evasion to Risk & Regulatory Team, MLRO, our line manager or Internal Audit.

Why is this important?

- As individuals, it is also illegal for us to help anyone evade tax. PIAS can be held criminally liable if we allow employees, or any other person associated with the company, to deliberately and dishonestly assist someone to evade tax. This could be a customer, supplier, business partner or other external party that has criminally evaded tax – we need to be able to show that we have not 'facilitated' that evasion.

For example:

- an employee accepts and processes an application from a customer knowing it declares a false tax residency which benefits the customer from a tax perspective
- a claims handler approves and processes a claim for a corporate customer, who requests the proceeds are paid into a personal bank account, so the "they don't have to tell the tax people"
- an employee knowingly agrees to break a large commission payment into multiple smaller payments over move that one tax period to help the intermediary hide their true tax liability

PIAS has procedures in place to ensure that where a potential incident of the facilitation of tax evasion has been identified, it must be referred to Risk & Regulatory Team or MLRO, our line manager or Internal Audit. This includes incidents of internal malpractice or dishonesty relating to the facilitation of tax evasion.

As part of any investigation markets must undertake a root cause analysis of the incident to determine any lessons to be learnt and whether any changes to systems, controls, policies and procedures are required to reduce the likelihood of an incident reoccurring. This must include re-visiting the facilitation of tax evasion risk assessment and undertaking deep dives into specific aspects of the incident such as the associated person due diligence.

All actual incidents of facilitation of tax evasion (those that are proven, substantiated or otherwise believed to be factual) must be reported to Group Financial Crime.

If at any time during an investigation of a facilitation of tax evasion incident, it is suspected that an individual or entity has evaded tax (including a tax saving), the monetary benefit would be deemed to be criminal property and they may have committed a money laundering offence. Similarly, any associated person who has facilitated the tax evasion may also have committed a money laundering offence. In either situation, a suspicious activity report must be submitted according to local procedures.

8.3 Suspicious Transactions or Unusual Activity Reporting - External

All employees and Representatives shall keep in mind of their obligations to report suspicious transactions as required by section 45(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.

When assessing whether a transaction is suspicious, PIAS considers the circumstances relating to the transactions in totality particularly where it appears unusual or does not make economic sense. PIAS also considers cases where they were unable to complete the CDD, simplified CDD or enhanced CDD measures, and where the customer concerned was reluctant, unable or unwilling to provide any information requested by the business and subsequently decides to withdraw a pending transaction or account application or terminate an existing business relationship.

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

Risk & Regulatory Team evaluates and document the basis of their determination in the Suspicious Transactions Register whether a matter should be referred to STRO within 15 business days and extend a copy to the Authority for information, 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. PIAS' Designated Individual or Nominated Officer will review the report before it is submitted to Singapore Police Force via STRO Online Notices and Reporting Platform (SONAR).

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

“Tipping Off” offence

During training, employees are taught not to do or say anything that might “tip off” another person that an internal or external report of (suspected or actual) money laundering or terrorist financing has been made. There are appropriate procedures to ensure employees do not otherwise prejudice a money laundering/terrorist financing investigation, even where an internal or external report has not been made.

Under Section 57 of the CDSA, the consequences for tipping off are:

- for an individual, a fine not exceeding S$250,000, or imprisonment not exceeding 3 years, or both; and

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

8.4 Sanctions Reporting

There are policies, procedures, systems and controls to identify, record, retain and report sanctions exposure internally and where necessary externally.

Further details are documented in the Sanctions policy.

Recording Sanctions Target Matches and Exposure – Sanction Exposure Register

There is a sanction register of relationships maintained with sanctions targets. This applies to all sanctions target matches identified, regardless of whether the sanctions are applicable in that jurisdiction or whether the relationship is held under a licence from the relevant authority, or other exception.

The register is kept up to date and is available to the Head of Risk Management & Compliance and Group Financial Crime on demand.

The Register must also be used to record any identified relationships that otherwise introduce sanctions risk to the business.

External Sanctions Reporting

No external reporting (including to regulators or law enforcement) of actual or suspected sanctions breaches may occur without first liaising with Head of Risk Management & Compliance to ensure that any local or Group external reporting is coordinated.

Any other external reporting or disclosures relating to sanctions, including external reporting of confirmed sanctions matches, must be approved by the Head of Risk Management & Compliance. PIAS may report to the regulators at any time. We do not have to report to Singlife before doing so and we can also report through both channels simultaneously.

8.5 Fraud Loss Reporting

PIAS documents and implements external reporting procedures based upon local regulatory, legislative, industry body, and government agency reporting obligations for external fraud losses.

PIAS has a responsibility to prevent, detect, report and investigate all instances of external fraud in accordance with Group's approach to financial crime. This must be supported by accurate and meaningful management information. As part of the investigation process, all fraud losses must be quantified to enable the reporting of material losses.

Where the investigation of a suspected external fraud incident indicates that PIAS' liability may exceed SGD 50,000, the case must be referred to the Risk & Regulatory Team who must consider whether further action is appropriate.

PIAS escalates to Group where appropriate, particularly where there may be wider implications or there are potential external reporting requirements.

8.6 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 Charter (by email, telephone or website)), suspicions or alleged instances of internal and non-customer malpractice or financial crime, including possible breaches of the Business Ethic Code.

In order to achieve this, PIAS reports such incidents to Internal Audit as soon as practical.

8.7 Speak Out Charter

Speak Out Charter is a confidential reporting process to enable PIAS employees, contractors, outsourced providers and other third party/ies to report behaviour in the workplace that may be a

breach of Group's 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.

9 Compliance Monitoring

PIAS has a risk-based compliance monitoring plan 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 the 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.

10 Training

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

Where additional training is required for departments that has high risk of financial crime, tailored training will be provided.

On an annual basis, Financial Crime training materials are reviewed and updated 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.

11 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 ('MI') is presented to Group Financial Crime Team monthly, using Group Financial Crime MI pack conforming to the format, template and requirements set by the Group Financial Crime Team.

12 Board and Management Reporting

The Risk and Regulatory team will 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's Financial Crime preference statements, the effectiveness of risk mitigating controls and any material matters such as regulatory violation together with the remediation actions.

13 Access to Customers' Personal Data

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

PIAS will not be required to provide an individual customer, beneficiary of a life insurance policy, an individual appointed to act on behalf of a customer, a connected party of a customer or a beneficial owner of a customer with:

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

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