Prevention of the Facilitation of Tax Evasion Policy

2024

Version Control

Revision Date	Version	Amendments	Author	Approver
01/06/2020	1	First Issuance to align to the Minimum Compliance Standards	Kelly Lam/ Frankie Tan/ Kenneth Goh	PIAS Risk Committee
19/10/2022	2	Review of Policy	Tang Ming Yang/ Chua Mei Na	PIAS Risk Committee
08/11/2023	2.1	Review of Policy	Tang Ming Yang/ Maisuri Abdul Karim	PIAS Risk Committee
30/11/2024	2.2	Review of Policy	Tang Ming Yang/ Maisuri Abdul Karim	PIAS Risk Committee

TABLE OF CONTENTS

1 Overview

1.1 Applicable Legislations

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

Frequency

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

1.2 Singlife Group Financial Crime Policy

PIAS has a legal, moral and social responsibility to its customers, shareholders and employees to deter and detect financial crime. Therefore, PIAS has no appetite for intentional or repeated breaches of law, regulation or policy related to financial crime, including acts of facilitation of tax evasion.

PIAS has a duty to comply with all legislative and regulatory requirements applicable to the jurisdiction in which it operates.

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

1.3 Top-Level Commitment

PIAS Senior Management promotes an ethical and compliant culture to deter acts of financial crime. This includes enhancing awareness, reinforcing understanding of employees' personal responsibilities under the Singlife 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 Singlife Group's approach to financial crime in line with Financial Crime Risk Preference Statements and Singlife Group's Business Ethics Code at least annually. Such communication shall explain Singlife Group's approach to financial crime; explain the consequences of breaching Singlife Group's standards; contain a commitment to carry out business fairly, honestly and openly; include information on how to report financial crime; highlight mechanisms for confidentiality raising concerns through whistleblowing (e.g. Singlife 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 Statement 3: Facilitation of Tax Evasion

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

PIAS has no appetite for acts of intentional facilitation of tax evasion by employees, representatives or other persons associated to PIAS.

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.

1.5 Employee Culture

The Head of Risk Management & Compliance ["RM&C"] shall ensure that all employees acknowledge and commit to Singlife 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 Singlife 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.

Communication from Singlife Group Financial Crime is also available on Singlife 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 Singlife Group's approach to financial crime risks and has implemented appropriate procedures to mitigate these risks.

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

Singlife Legal Counsel ensures 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 Singlife Group's approach to financial crime.

In addition, in areas where PIAS identifies as being higher risk of exposure to financial crime, PIAS will consider issuing additional external communications to embed Singlife Group's approach to financial crime risk and consequences for non-compliance as well as raise awareness of expected Singlife Group financial crime compliance standards, procedures and 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 ["RM&C"] identifies and documents any local regulatory or legal requirement for public disclosure of PIAS' approach to managing their financial crime risks.

All public disclosures of matters relating to financial crime risk management (including publication on an external PIAS website) will be approved by Singlife Group Financial Crime.

2 Governance & Accountabilities

2.1 Governance Committee

PIAS Risk Committee, is tasked with the responsibility to provide adequate oversight over the management of financial crime risk.

2.2 Governance Responsibilities

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 money-laundering/terrorism financing (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.

PIAS Risk Committee provides oversight on the 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 Singlife Group Head of Legal & Compliance on any known any financial crime breaches, control failures, issues and risks outside tolerance.

In addition, PIAS Risk Committee reviews and approves 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 Singlife Group Financial Crime.

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

2.3 The Three Lines of Defence Operating Model

Roles and responsibilities of Three Lines of Defence

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

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

Roles and responsibilities include:

- Risk identification, ownership, management and control, including a supportive risk culture

- Executing the requirements of an adequate and appropriate Financial Crime Risk Management Framework
- Escalations to Risk & Regulatory Team (including appropriate reporting) where required in a timely, transparent and open manner
- Apply and execute the Singlife Group Financial Crime Policy to and on their Business Area
- Support a resourcing model adequate and appropriate to maintaining a Financial Crime Risk Management Framework
- Develop open communication channels with 2nd LOD to ensure specialist support, advice and guidance is obtained from financial crime compliance experts as required
- Partner with 2nd LOD to design and implement an assurance testing strategy and framework for all financial crime controls
- Ownership of all data

The business operations are responsible for the implementation of robust controls to identify, assess and mitigate financial crime risks and escalate any red flags to PIAS' Risk & Regulatory team.

Policies, procedures and controls to mitigate financial crime and especially those specific to ML/TF should be clearly documented and communicated to all relevant officers, employees and agents in the various business units. All employees are required to undergo annual financial crime training (minimally covering ML/TF) so that they are aware of the latest trends and developments and the related regulatory obligations for their compliance.

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

- Risk Management & Compliance ["RM&C"]

Roles and responsibilities include:

Strategy

- Define and implement a Financial Crime Risk Management Framework
- Provide insight, advice and guidance to the Singilfe 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 management information ("MI") reporting framework

- Support a resourcing model to fulfil the Singlife 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 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 for formulating and reviewing the risk-based financial crime risk management framework as well as ongoing monitoring of the relevant internal controls. This includes screening of new and existing business relations, ongoing monitoring and review.

The Risk & Regulatory Team is also 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 Singlife Group Head of Legal & Compliance is responsible for escalating any material financial crime related risks or regulatory breaches to the Singlife Group CEO and to the Board Risk Committee.

Third line of defence (3rd LOD): Internal Audit
- Internal Audit

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

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.

2.4 Financial Crime Programme

The Designated Individual puts in place an appropriate Financial Crime Programme which ensures 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)
- 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 Singlife 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 and where required, escalation to Singlife Group Financial Crime, MAS and/or other relevant authorities. Perform risk assessment and report any true matches in Global Name Screening ('GNS') for all categories (i.e. sanctions, Politically Exposed Persons and "High" or "Very High" Risk Countries based on Jurisdiction Index) to Singlife 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 reviews 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 is documented at PIAS Risk Committee.

2.6 Notification of Appointments

PIAS provides to Singlife Group Financial Crime, the details of the individuals appointed as its Designated individual, MLRO and Nominated Officer.

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

2.7 Appointment of a Designated Individual

PIAS's Chief Executive Officer (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 if 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's CEO shall ensure 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 Singlife Group Financial Crime, together with a plan for resolution. For PIAS, the Designated Individual is the Head of Risk Management & Compliance ["RM&C"].
Where any conflicts and the responsibilities of the AML/CFT Compliance Officer arise, the matter must be escalated to the Singlife Group Head of Legal & Compliance who will ensure that the AML/CFT concerns are objectively considered and addressed.

2.8 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 the business/market/cell 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 PIAS as well as assessing and reporting on the adequacy of the financial crime risk management 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.

2.9 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's 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 Singlife Group so that the financial crime risks exposure may be evaluated. The enterprise-wide financial crime risk assessment will enable the Singlife 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 Singlife 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 Singlife Group's enterprise-wide ML/TF risk assessment.

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

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

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

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

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

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

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

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

3.2 Identifying, Assessing and Understanding Financial Crime Risks

PIAS identifies, assesses and understands the respective financial crime risks in relation to:

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

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

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

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

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

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

3.3 Product Developments, Practices, Technologies and Customer Proposition Initiatives

On a regular basis (at least annually), PIAS assesses the risk of 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 Singlife Group's requirements. The Head of Risk Management & Compliance ["RM&C"] ensures that financial crime risks are addressed during the new product development process by implementing appropriate measures to manage and mitigate the risk in accordance with the risk-based approach.

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 escalated to Singlife 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 ["RM&C"] will present the proposal and the risk assessment to Singlife 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 Singlife Group Head of Legal & Compliance approval is required prior to launch.

3.4 Mergers and Acquisitions

The Head of Risk Management & Compliance ["RM&C"] 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 Singlife Group's mergers and acquisitions processes.

The risk assessment is documented and considers 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 business especially where the firm's processes and procedures are below the requirements of Singlife 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 Singlife 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 ["RM&C"] uses Enterprise-Wide Risk Assessment (EWRA) and any other assessments of financial crime risk to design, implement and operate effective and proportionate controls to mitigate financial crime risks.

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

- customer due diligence (including enhanced due diligence and associated person (non-customer) due diligence)
- screening
- ongoing monitoring
- compliance monitoring
- training

The risk-based approach is documented (either as a stand-alone document or incorporated in other relevant documents) and is in consideration of the Singlife Group Financial Crime Policy. The approach will be reviewed at least annually to ensure continued suitability.

4 Facilitation of Tax Evasion

4.1 Definition and Examples

Tax Evasion is the illegal non-payment of taxes due. Facilitation of tax evasion is knowingly assisting an individual or firm to evade tax.

Though tax evasion is most commonly linked to corporate income tax, it can also involve the Goods and Services Tax (GST), or personal income tax. The Monetary Authority of Singapore has also designated a broad range of serious tax crimes as money laundering predicate offences, from 1 July 2013 onwards.

Some examples of how customers or suppliers may possibly evade tax:

- An individual does not declare income from an offshore investment to the tax authorities, evading tax
- An investor deliberately falsifies an annual statement of their investments to report a lower amount of income to the tax authorities to pay less tax
- A supplier provides goods, but gets paid for them in cash (or to a non-business account) and does not account for it in their tax return

PIAS must not be involved in any direct or indirect facilitation of tax evasion with its employees, agents, suppliers, business partners, directors, intermediaries etc.

Examples of acts of facilitation of tax evasion

- an employee accepts and processes an application from a customer knowing it declares a false tax residency
- 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 an intermediary hide their true tax liability
- a broker selling deliberately sells tax-efficient products to those not entitled to the product, by disguising their tax residency by using their own address

4.2 Seriousness of Facilitating Tax Evasion

PIAS has a moral and legal responsibility to ensure that we are not enabling anyone to use us, our services, or our products to evade tax. If anyone acting on behalf of PIAS (including employees) uses PIAS's products or services to assist an individual or firm to evade tax, it could lead to criminal prosecutions for PIAS and the individual(s) who facilitated the tax evasion.
Section 96 of the Income Tax Act 1947 penalizes tax evaders with 3 times the amount of tax undercharged, and/or $10,000 fine and/or 3 years of imprisonment, if convicted.

5 Due Diligence

5.1 Associated Persons and Non-Customer Definitions

An associated person is defined as an employee, an agent or any other person who performs services on or behalf of the person (i.e. PIAS). The term encompasses a wider range of persons connected to PIAS who might be capable of facilitating tax evasion on its behalf.

PIAS is liable for the corporate criminal offence of failing to prevent the facilitation of tax evasion when a person associated with it, acting as someone so associated, has criminally facilitated tax evasion, unless it can prove it had in place reasonable prevention procedures to prevent that person's criminal act.

The definition of an associated person is intended to be broad in scope, being dependent on the facts of the case. It therefore captures all person who might be capable of the facilitation of tax evasion whilst acting on behalf of PIAS, including (both permanent and temporary), intermediaries, suppliers, business partners, outsourced services, offshore centres, group companies and joint ventures. These would be treated as an associated person where they provide services “for or on behalf” of PIAS.

5.2 Employees - Recruitment

Singlife People Function provides shared human resource services to PIAS including recruitment of employees. PIAS’ new employees (both permanent and temporary, including contractors) are hired objectively and thoroughly screened prior to employment in line with Singlife 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 Singlife 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 Singlife which will include Sanctions, Politically Exposed Persons (PEPs) and Special Interest Persons (SIPs) screening using Global Name Screening tool (GNS).

5.3 Employees – Post Recruitment

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

Employees’ names are screened daily in the GNS system to detect any PEP, Sanctions and adverse news.

PIAS needs to identify all the 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 ensures that all employees attest annually to Singlife Group’s Business Ethics Code.

5.4 Mergers and Acquisitions (M&A)

When PIAS is undertaking an acquisition, merger or joint venture, PIAS ensures that the target company has been subjected to suitable financial crime due diligence, including specifically ensuring it has an adequate financial crime control framework and is able to evidence its effective operation. This includes M&A and joint venture transactions.

Any identified financial crime related gaps in compliance will be escalated to the relevant committee overseeing the merger/acquisition, with a recommendation from the Risk & Regulatory Team on whether to proceed with the transaction. This may include identifying the need for subsequent financial crime control enhancements by the target entity to ensure compliance with PIAS financial crime risk appetite and tolerances.

PIAS ensures that when third parties are engaged to assist with any merger, acquisition or joint venture transaction (e.g. intermediaries, local representatives, introducers, negotiators, etc.), these third-parties are subjected to appropriate financial crime due diligence themselves. This may require the introduction of further financial crime controls, such as requiring financial crime related representations, warranties in legal documentation and specific undertakings to comply with PIAS's financial crime requirements given that PIAS could become criminally liable for non-compliance in the area of bribery, corruption and facilitation of tax evasion.

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

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

A risk rating framework is established and applied to non-employee associated persons and third-party relationships, which records the status of the relationship, assesses and records the risk of facilitation of tax evasion associated to each relationship. For associated persons providing services "for or on behalf" of PIAS, this data must be stored within an associated persons register which records relevant details and establishes appropriate levels of due diligence.

At a minimum, the register must include the following:

- the proposed role of the associated person and the nature of the relationship being provided
- the country or location of the associated person
- the amount of proposed consideration or payment to the associated person and whether it is proportionate to the tasks required and/or in line with market rates
- the transparency and reputation of the associated person, including their relationship with regulators, public officials or government agencies
- the presence of a potential conflict of interest (e.g. a party involved may be a friend or relative of an employee who facilitates or advises on a service/relationship)

5.6 Due Diligence, Screening and Documentation for Non-Employee Associated Persons and Other Third-Party

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

Where the non-employee associated person is an entity other than a natural person, for example a company, the key corporate personnel and beneficial owners are identified and screened as well. The identification procedures for key corporate personnel and beneficial owners should be equivalent to the identification (but not verification) requirements required for a similar entity under the relevant local AML requirements.
Confirmed true name match from screening is assessed and approval from PIAS's Chief Executive Officer (CEO) is sought before business relationship is established.

Copies of due diligence materials, including risk assessments, the results of screening, and any referrals to Risk & Regulatory Team or governance committees are retained for at least 7 years.

5.7 High-Risk Third Parties and High-Risk Non-Employee Associated Persons – Financial Crime Review and Approval (Facilitation of Tax Evasion)

The Risk & Regulatory Team reviews and assesses the following relationships:

- all 'high risk' non-employee associated persons
- any non-employee associated person or third-party which has been linked to facilitation of tax evasion

The nature and scope of the non-employee associated person or third-party business relationship is reviewed by Risk & Regulatory Team and prior to the establishment of the relationship, approval from PIAS's CEO is sought. Any additional controls required to mitigate the facilitation of tax evasion risks associated with the arrangement are documented.

PIAS will not establish a business relationship with a high-risk third-party or high-risk non-employee associated persons without the approval from PIAS's CEO and PIAS Risk Committee.

The assessment of the facilitation of tax evasion risks associated with the business relationship, the decision made and the detailed rationale behind the decision made are documented.

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

6 Name Screening

6.1 PEPs Screening

PIAS identifies Politically Exposed Persons ("PEPs") relationships to appropriately manage the potential increase in risk exposure to tax evasion, bribery etc.

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 PEPs and their association to financial crime. (Note: Any decision not to screen customers/ counterparties/clients are documented and agreed by PIAS Risk Committee.)

Screening is conducted using GNS at the initiation stage and on an on-going daily basis throughout the business relationship.

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

All PEPs are considered High-Risk Customers and approval is sought from PIAS's CEO before a business relationship is formed. Thereafter they are placed on the PIAS's High-Risk Customers list and tagged in Vue system with appropriate tagging codes for on-going monitoring.

6.2 Additional Screening

PIAS identifies and manages 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 Singlife 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 Singlife Group's Jurisdiction Index.

6.3 State-Owned Companies (SOC) Screening

Through screening relevant in-scope customer and non-customer relationships, PIAS seeks to identify a connection or relationship with state-owned company or state-owned company executive and appropriately assess and manage the financial crime risk involved (such as risk of

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

People and parties to be screened includes but not limited to:

- All customers (individuals and corporate), beneficial owners of the customer and beneficiaries. For corporate customers, it includes identified key corporate personnel.
- All non-employee associated persons (i.e. an agent or any other person who performs services or acts for or on behalf of PIAS who are not PIAS employee or customer). For entity other than a natural person, it includes identified key corporate personnel and beneficial owners.
- Target or counterparty of any corporate acquisition or disposal (including Joint Venture Partners)
- All employees
- Connected parties etc.

Screening takes place at the initiation stage and on an on-going daily basis throughout the business relationship using Global Name Screening (GNS) system. Alternative or additional methods (e.g. one-time internet research or bespoke due diligence reports) may also be used by the Risk and Regulatory Team to aid in customer due diligence.

PIAS clears SOC alerts within 30 business days and ensures the appropriate actions are taken.

When PIAS identifies a connection to a SOC, the Risk and Regulatory team assesses the financial crime risk of that relationship and documents the decision to establish, retain, reject or end the relationship. Approval is sought from PIAS's CEO before a business relationship is formed. Thereafter they are placed on the PIAS's High-Risk Customers list and tagged in Vue system with appropriate tagging codes for on-going monitoring.

7 Record Keeping

Record retention and retrieval

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

- documents and information obtained to satisfy CDD requirements (e.g. identification documents/certificates, proof of address, EDD documents etc.)
- records relating to customer transactions
- documents relating to the review/investigation of potentially suspicious or unusual activity
- records relating to training (i.e. date of completion, nature of training, attendance records etc.) and compliance monitoring (i.e. reports to senior management)
- records of screening and potential match investigation
- risk assessments and FCRMP documents
- incident investigation reports

PIAS shall ensure compliance with the record retention period set out in paragraph 10 of the MAS FAA Notice 06 on Prevention of Money Laundering and Countering the Financing of Terrorism - Financial Advisers ("FAA-N06").

At minimum, the following retention period should be complied:

- 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 retains 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 Singlife 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.

8 Ongoing Monitoring

8.1 Transaction Monitoring

PIAS is responsible for monitoring transactions related to PIAS' activities on an ongoing basis to help identify unusual activity which may be connected to financial crime or tax predicate offences. Transaction monitoring is performed in accordance with requirements determined by the relevant MAS Notice and other AML/CFT laws, regulations or applicable Notices in Singapore.

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

The transaction monitoring framework and thresholds are documented, approved by the Designated Individual and endorsed by PIAS Risk Committee and reviewed at least annually.

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

8.2 Monitoring and Review Scenarios - Facilitation of Tax Evasion

PIAS identifies and documents scenarios relevant to its business, location and products/services that may be indicative of the facilitation of tax evasion. These scenarios will inform the extent and nature of transaction monitoring.

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

- facilitation of tax evasion threats, typologies and examples identified in local national risk assessments, law enforcement publications or regulatory guidance
- typologies identified by international organisations, such as Financial Action Task Force
- life wrapper products (where 'private' investments are tied to the policy and not the individual, and hence not declared as investment income)

- clients purchasing excessively large policies who are non-resident or using onshore or offshore trust accounts
- non-resident customers from countries with higher tax rates, particularly where the product involves investment assets which are located in the customer jurisdiction;
- business involving countries with higher risk of tax evasion or the facilitation of tax evasion
- third-party has deliberately failed to register for GST (or the equivalent tax in any relevant jurisdiction outside Singapore) or failed to account for GST;
- third-party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;
- third-party service provider requests that invoice is obtained from or payment is directed to a third-party who is not party to the service contract;
- an employee asks to be treated as a self-employed contractor, but without any material changes to their working conditions; third-party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us
- third-party requests that payment is made to a country or geographic location different from where the third-party resides or conducts business;
- invoiced for a commission or fee payment that appears too large or too small, given the service stated to have been provided
- third-party to whom we have provided services requests that their invoice is addressed to a different entity or person, where we did not provide services to such entity directly
- receive an invoice from a third-party that appears to be non-standard or customised

Scenarios are based on PIAS' risk profile, takes into account the output from the relevant financial crime risk assessments, and the above minimum scenarios will only act as an aide memoire to assist in documenting the transaction monitoring framework.

8.3 Identifying Relevant Activity – Facilitation of Tax Evasion

PIAS uses identified facilitation of tax evasion scenarios to identify and document activity for monitoring. At a minimum, PIAS will seek to identify activities that are deemed to pose a higher risk of facilitation of tax evasion and introduce suitable monitoring.

Examples include but are not limited to:

- payments out to unidentified third parties (e.g. claims settlement to a limited company being paid to an individual)
- multiple supplier payments in response to a single invoice (incl. different payment dates, different accounts, different jurisdictions)
- multiple funding sources (e.g. different parties, different jurisdictions etc.) for a single product/service
- single funding source for multiple products/services held in different names
- changes to payment source or destination (e.g. change of supplier bank account, changes to beneficiary's country of residence)

- complex or unusual transaction patterns, especially those requested by the customer/supplier/third-party (e.g. staggered payments, delayed payment, re-assignment of benefit/asset ownership etc.)
- cash payments/transactions (including to and from suppliers and third parties)

The above are only examples of potentially higher risk activities and must not be considered as the only examples. An assessment must be undertaken locally to determine the relevant activity.

Transaction monitoring for the facilitation of tax evasion will form part of the transaction monitoring framework which must be approved by PIAS Risk Committee.

9 Risk Reporting

9.1 Suspicious Transactions or Unusual Activity Reporting

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

If an employee or Representative has suspicion 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, he shall immediately refer the matter to the Designated Individual i.e. PIAS' Head of Risk Management & Compliance ["RM&C"].

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.

PIAS educates employees regularly where a suspected facilitation of tax evasion incident has been identified, it must be referred to Internal Audit using 'Speak Out Charter' or the Risk or Regulatory Team. This includes requests for a bribe, such as facilitation payments, even if the request is refused.

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

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

The suspected facilitation of tax evasion incidents must be reported to the Singlife Group Financial Crime Team.

9.2 External Reporting of the Facilitation of Tax Evasion Incidents

Where the investigation of a suspected facilitation of tax evasion incident identifies an actual incident of the facilitation of tax evasion (those that are proven, substantiated or otherwise believed to be factual) these must be reported to the Singlife Group Financial Crime (if not already reported as a 'potential' case).

Singlife Group Financial Crime will review the findings of the investigation, liaise with appropriate stakeholders (such as Legal, People Function, the company or business unit concerned, Operational Risk Committee and Board Risk Committee) to determine the extent of external reporting required.

9.3 "Tipping-Off" Offence

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

This must include consideration of the following:

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

"Tipping-off" does not include disclosures to regulators/supervisors, other 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 the Head of

Risk Management & Compliance ["RM&C"] who may then escalate to Group Financial Crime Team, where appropriate.

9.4 Incident Reporting

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

To achieve this, PIAS identifies and reports such incidents to Internal Audit as soon as practicable.

9.5 "Speak Out Charter"

"Speak Out Charter" is a confidential reporting process to enable PIAS employees, contractors, outsourced providers and other third-parties to report behaviour in the workplace (by Singlife or Third Parties) that may be a breach of Singlife 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 Singlife Group's Business Ethics Code.

10 Compliance Monitoring

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

The scope, nature and frequency of monitoring are documented as part of the annual 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.

10.1 Compliance Monitoring - Resources

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

The Risk & Regulatory Team must have full, free and unrestricted access to all business activities, records, data, property and personnel necessary to complete their work. The Risk & Regulatory Team is specifically responsible to oversee compliance of the financial crime activities.

Any identified gaps in capacity, capability or access are escalated to PIAS Risk Committee and Singlife Group Financial Crime.

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

10.2 Compliance Monitoring – Findings and Remediation

The findings from any financial crime compliance monitoring review are fully documented and reported to the Designated Individual(s), PIAS Risk Committee and to Singlife Group Financial Crime.

Any identified issues are included within MetricStream (or equivalent) along with appropriate action plans and assigned owners to support closure.

Both 1st and 2nd LODs are expected to take all appropriate action to remedy any deficiencies identified through compliance monitoring reviews and report on the progress of such activities to PIAS Risk Committee. Any deficiencies identified that are not being given appropriate attention must be escalated to Singlife Group Financial Crime.

11 Response to Financial Crime

To manage financial crime incidents in a coordinated and informed manner, the relevant business unit is expected to document the actions that will be taken in response to specified financial crime events. This will include documented procedures for the receipt, review and response to requests, enquires or notices from law enforcement agencies and relevant regulatory/governmental authorities.

The plan (or the components that make up the plan) is the responsibility of the Designated Individual and will be approved by the Designated Individual and PIAS Risk Committee on an annual basis (or more frequently if any changes are made to the plan). It is reviewed and, if necessary updated, in the event of any changes to process following a financial crime incident or relevant changes to the financial crime risk assessments.

The scope and nature of the procedures, including any specific legal or regulatory requirements, will be included as part of the Financial Crime Programme and be proportionate to the volume, frequency and nature of financial crime incidents and requests received.

PIAS also complies with Section 35 of the Criminal Procedure Code 2010 on ‘Powers to seize property in certain circumstances’ when responding to financial crimes.

12 Financial Crime Training and Awareness

The Head of Risk Management & Compliance [“RM&C”] ensures that all employees acknowledge and commit to Group’s approach to financial crime risks. Training is provided (as part of their induction) through the Essential Learning / Learning Management System for existing and new

employees, permanent or temporary contract workers, including contractors are tested yearly. PIAS employees are reminded any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly.

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

On an annual basis, Financial Crime training materials are reviewed and 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 take appropriate action against those who are unable to complete the AML/CFT training without a reasonable cause.

13 Management Information ("MI")

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

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

14 Board and Management Reporting

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