Sanctions Policy

2024

Version Control

Revision Date	Version	Amendments	Author	Approver
01/06/2020	1	First Issuance to align to the Minimum Compliance Standards	Frankie Tan	PIAS Risk Committee
18/8/2020	1	Insertion under Any Other Relevant Parties in Section 4.1 Who Must Be Screened the phrase third party non customer payee	Kelly Lam	PIAS Risk Committee
10/10/2022	2	Annual Updates	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee
07/11/2023	2.1	Annual Updates	Tang Ming Yang / Maisuri Abdul Karim	PIAS Risk Committee
14/06/2024	3	(i) Insertion of Section 2.3 Proliferation Financing Typologies/Indicators, (ii) Expansion of Section 2 Introduction to Sanctions (iii) Insertion of Section 8.1 Lookback Mechanism	Tang Ming Yang / Chua Mei Na	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 Group Financial Crime Policy, and all applicable regulations that may be issued by the relevant authorities in Singapore. Targeted financial sanctions are governed by the financial sanctions issued by the Monetary Authority of Singapore ("MAS").

1.2 Frequency

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

1.3 Group Financial Crime Policy

PIAS has a legal, moral and social responsibility to its customers, shareholders and employees to deter and detect financial crime. Violations of laws and regulations relating to financial crime may result in criminal, civil or regulatory penalties for PIAS, 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 PIAS, 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
- 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 client, 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 the senior management

on reasonable grounds and needs to be in line with the Group Financial Crime Policy and all applicable regulations. Such waiver or deviation shall be reported to Singlife Group Financial Crime on a quarterly basis.

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 noncompliance. 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.

1.4 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 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 the 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.

1.5 Risk Preference Statements

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

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) Special Risk Countries

As a general principle, PIAS has no appetite for conducting business in, involving, with, or on behalf of, customers and counterparties based in or customers or counterparties from very high risk rated special risk countries without an appropriately approved and permissible exception. PIAS has limited appetite for conducting business in, involving, with, or on behalf of, customers and counterparties based in or from high risk rated special risk 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 inducements to or from public officials the payment of inducements to public officials by an employee or Financial Adviser Representative or providing facilitation payments.

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

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 limited appetite for conducting business with restricted customers 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.

1.6 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 ("LMS") / Essential Learning Course. The annual attestation via the LMS or 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.

On an annual basis, employees are required to acknowledge the Group Business Ethics Code.

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

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

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

1.7 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 the 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 of 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.

1.8 External Communications

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

1.9 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.

1.10 Governance Responsibilities

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

In addition, PIAS Risk Committee will review and approve any financial crime policies and procedures as well as approve the approach 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 Introduction to Sanctions

Sanction is defined as an official order, such as the stopping of trade, that is taken against a country in order to make it obey international law. It includes a wide range of restrictive/coercive measures. They can include arms embargoes, travel or investment bans, financial sanctions (primarily asset freezes), reduced diplomatic links, reductions / cessation of any military relationship, flight bans, suspension from international organizations, withdrawal of aid, trade embargoes, restriction on cultural /sporting links, etc. Sanction is usually imposed with the goal of changing the behaviour of the target. For example, to penalize states for violating international law, to force a change in policies related to human rights or nuclear proliferation, or counter-terrorism or organized crime, to change the behaviour of a regime and to promote democracy, peace, and stability in a region.

Proliferation is defined by the Financial Action Task Force (FATF) as the illegal manufacture, acquisition development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

2.1 Types of Sanctions

Sanctions are divided into 2 categories:

I. <u>Financial Sanctions</u>

Restrictions put in place by the UN, EU or UK and other national governments to achieve a specific foreign policy or national security objective. They can either limit the provision of certain financial services or restrict access to financial markets, funds and economic resources.

II. <u>Trade Sanctions</u>

Include restrictions on exports implemented for political reasons by countries and international organizations to maintain international peace and security. Sanctions measures include arms embargoes* and other trade control restrictions.

** An arms embargo is a prohibition or sanction against the export of weaponry and dual-use items - goods which have both a civil and military use. This can include raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. Dual use goods could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers.*

2.2 Prohibiting Sanctions Circumvention

PIAS Money Laundering Reporting Officer ("MLRO"), who is also the Head of Risk Management & Compliance, and Risk & Regulatory Team ensures that as part of Employee Culture and sanctions training, all relevant employees are made aware that any attempts to circumvent sanctions could be a criminal offence and would be a breach of Group's Business Ethics Code and a disciplinary offence.

This includes specifically prohibiting circumvention of sanctions, for example by:

- omitting, deleting or altering information for the purpose of avoiding identification of sanctions risk
- structuring business or transactions with the purpose of concealing the involvement of a sanctioned party
- failing to escalate identified sanctions risk

The following are local penalties imposed in the event of sanctions circumvention:

- Financial Institution
  Under the Financial Services and Markets Act 2022 ("FSM Act"), a financial institution that contravenes any FSMregulations is guilty of an offence and will be liable on conviction to a fine not exceeding $1,000,000 for each offenceand in the case of a continuing offence, a further fine of $100,000 for every day or part of the day during which the offence continues after conviction.

- Natural Persons in Singapore

Under the United Nations Act 2001 ("UN Act"), a person who commits an offence against any Regulations made under the UN Act will be liable on conviction, in the case of an individual, to a fine not exceeding $500,000 or to imprisonment for a term not exceeding 10 years or to both; or in any other case, to a fine of up to $1 million.

2.3 Proliferation Financing Indicators/Typologies

- The customer's transaction involves an individual or entity in a foreign country associated with proliferation and/or sanctions evasion concern;
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of persons who have been denied export licences, or has a history of export control contraventions;
- The customer's transactions involve possible shell companies (e.g. companies that do not appear to have real business activities in Singapore and display other shell company indicators);
- The customer is vague and resistant to providing additional information when asked;
- The customer has a sudden change in business activities.
- The customer is known or believed to have previous dealings with individuals or entities in countries subject to UNSC sanctions; or
- Sudden/frequent changes in directorship/authorised signatories which are not well-explained or intended to conceal links with individuals associated with sanctioned countries/activities.
- The customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;
- The transaction involves designated persons;
- The transaction involves higher risk jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;
- The transaction involves other financial institutions with known deficiencies in AML/CFT controls or controls for combating proliferation financing;
- The transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators).

3 Customer Due Diligence & Enhanced Due Diligence

3.1 Customer Due Diligence ("CDD")

PIAS following the requirements for CDD contained in the Anti-Money Laundering and Counter Terrorist Financing policy in order to ensure that accurate and complete information is available for name screening and that sanctions risk can be fully assessed.

PIAS uses the Global Name Screening ("GNS") system to ensure that additional CDD measures are taken to protect PIAS from breaching sanctions where the customer is known to do business with (or otherwise engage with) sanctioned targets or countries subjected to sanctions; or the

customer otherwise carries a higher sanctions risk (e.g. produces goods subject to sanctions or export controls, transports goods to/from a sanctioned country).

3.2 Additional Customer Due Diligence ("CDD")

Additional CDD measures include:

- Increasing the scope and depth of CDD
- Increasing the frequency of CDD refresh
- Obtaining and assessing specific information on the nature, extent and type of the customer's business involving sanctioned parties and countries through Enhanced Due Diligence Form
- Obtaining and assessing information from the customer on their measures to maintain compliance with sanctions
- Obtaining and considering specific legal advice on the relationship
- Obtaining additional internal approval and/or risk-acceptance of the relationship

3.3 Enhanced Due Diligence ("EDD")

PIAS follows the requirements for Enhanced Due Diligence (EDD) contained in the Anti-Money Laundering and Counter Terrorist Financing policy if we establish or maintain business relationships with customers identified as high-risk, as a result of sanctions risk. This includes the following:

- Where the customer (including any identified beneficial owner or key corporate personnel) is a sanctions target, they will be treated as a high risk customer and EDD must be conducted on retained customers.
- Where the customer is resident, incorporated, controlled from, or based in a country subjected to sanctions (included in very high or high risk countries listed in the Group's Jurisdiction Index ("JI")), they will be treated as a high risk customer and EDD must be conducted on retained customers.
- Where the customer draws 10% or more of its wealth, revenue or turnover from a country subjected to sanctions (included in very high risk countries in the JI), they will be a high risk customer and EDD must be conducted.
- Where the customer draws 25% or more of its wealth, revenue or turnover from a country subjected to sanctions (included in high risk countries in the JI), they will be treated as a high risk customer and EDD must be conducted.

In all circumstances where EDD is required as a result of sanctions risk (wholly or partially), the following additional measures may be applied:

- Increasing the scope and depth of CDD
- Increasing the frequency of CDD refresh
- Obtaining and assessing specific information on the nature, extent and type of the customer's business involving sanctioned parties and countries

- Obtaining and assessing information from the customer on their measures to maintain compliance with sanctions
- Obtaining and considering specific legal advice on the relationship
- Obtaining additional internal approval and/or risk-acceptance of the relationship.

3.4 Customers Retained Under License

In the event where the retention of customers subjected to Sanctions is approved by an official government license (or similar), the terms of such a license are adhered to. This also applies to any other similar official authorisation or approval for retaining customers subject to sanctions or otherwise interacting with Sanctioned parties, which also includes 'general' and specific licenses.

The process includes the following:
- Application for licenses/approval
- Maintaining compliance with licenses
- Timely renewal of licenses
- Oversight and approval of compliance procedures
- Compliance with Prohibited and Restricted Customers procedures
- Compliance with Sanctions reporting procedures

3.5 Activity Authorized Under License

In the event where PIAS undertakes activities involving sanctioned entities, countries or goods that are approved by an official government license (or similar), the terms of such a license must be adhered to. This also applies to any other similar official authorisation or approval for activities subject to sanctions or otherwise interacting with sanctioned parties, which also includes 'general' and specific licenses.

Examples of when this may occur include:
- Claim payment to a third-party subjected to sanctions, or in a sanctioned country
- Insuring the export of licensable goods subject to sanctions restrictions
- Insuring the shipment of humanitarian aid to a sanctioned country
- Acceptance of funds from a party subject to sanctions
- Acquisition of a book of business containing parties subject to sanctions

The processes put in place include:
- Validation of licenses/approval
- Maintaining compliance with licenses
- Oversight and approval of compliance procedures
- Compliance with Sanctions reporting procedures

3.6 Associated Persons

An associated person includes any person, corporate or individual that performs services for or on behalf of PIAS, which includes employees. The term encompasses a wide range of persons connected to PIAS who might be capable of breaching Sanctions or introducing Sanctions risk.

3.6.1 Employees – Recruitment

Singlife's People Function oversees hiring for PIAS. PIAS's 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 will be 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 (GNS).

3.6.2 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 the Group Business Code of Ethics.

3.6.3 Mergers & Acquisitions ("M&A")

When PIAS is undertaking an acquisition, merger or joint venture, PIAS ensures that the target company has been subject 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 by the Group M&A/Joint Ventures team.

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 Group's policy, appetite and tolerance.

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

3.6.4 Associated Person Sanctions Compliance

In addition to confirming that an associated person is not themselves subject to sanctions through appropriate associated person due diligence, PIAS considers the sanctions risk that an associated person introduces to PIAS and may introduce suitable mitigating actions.

This includes where a PIAS business delegates any underwriting or claims authority to a third-party or associated person, that business must satisfy itself that the party's systems and controls are aligned to Group's Risk Preference Statements and sanctions appetite. This may be achieved through:

- Making specific reference to sanctions compliance within any Terms of Business or contract
- Communicating PIAS's sanctions appetite and restrictions (and any changes to these) to delegate parties
- Requiring positive affirmation (e.g. 'representations and warranties') on sanctions compliance from the third-party/associated person
- Requiring a minimum set of information to be obtained from the underlying customer through the EDD Form and subjected to sanctions screening
- Restricting delegation to pre-approved business/activities/clients/etc
- Conducting suitable oversight and testing of delegated business

Any identified actual or potential breach of PIAS's sanctions risk appetite (even if not a breach of sanctions legislation/regulation) as a result of associated person activity on behalf of PIAS must be reported to Group Financial Crime.

4 Global Name Screening ("GNS")

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

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

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

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

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

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

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

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

a) immediately freeze funds, other financial assets or economic resources of the designated individual and entity;

b) abort entering into any financial transactions or provide financial assistance or services in relation to: (i) designated individuals, entities or items; or (ii) proliferation and nuclear, or other sanctioned activities;

c) inform MAS of any fact or information relating to the funds, other financial assets or economic resources owned or controlled, directly or indirectly, by a designated individual or entity; and

d) file a suspicious transaction report ("STR") and extend a copy to MAS

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

4.1 Who Must Be Screened

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

4.1.1 Screening of PIAS Representatives

All PIAS Representatives are screened prior to onboarding. PIAS Representatives identified as High-Risk based on Group's Jurisdiction Index are screened daily on an ongoing monitoring. Any form of new adverse information has to be investigated by Risk & Regulatory Team and if necessary, escalated to the Head of Risk Management & Compliance.

For PIAS Representatives, PIAS's Adviser Management Unit ("AMU") conducts initial screening and reference checks with respect to the candidate's integrity. Any possible matches are flagged and escalated to Risk Management & Compliance Department to conduct further review. The representative's name is included for daily screening via GNS. If any adverse findings are detected during subsequent screenings, it will be shared with the business for further assessment.

4.1.2 Screenings of Employees

Singlife's People Function conducts initial screening and reference checks with respect to the candidate's integrity. If the candidate's name is flagged out with adverse media or highlighted as a PEPs, this will be managed by Singlife's People Function, which includes notifying the relevant reporting Manager in PIAS. Employees are screened daily under batch screening via GNS. If any

adverse findings are detected during subsequent screenings, it will be shared with the business for further assessment.

4.1.3 Screening of (Natural Person) Customers

All (natural-person) customers must be screened at the initiation of relationship as well as upon any form of trigger events (for e.g. updates to address, name change, etc.). After successful on-boarding, daily ongoing screening is conducted for all existing customers. Assessment shall be based on the customer data that was uploaded into GNS. On a need-to basis, the Risk & Regulatory Team extracts customer data from database systems and utilize internet search engines to source for more information for hit discounting.

4.1.4 Screening of Corporate Customers

For corporate customers, the full legal name of the individual or entity (and any known alias) must be screened. This includes any identified key corporate personnel, beneficial owners and beneficiaries of long-term insurance contracts, other related counterparties, associated persons (including employees or businesses introduced by associate d persons)/connected parties and any other relevant parties identified during the diligence process. At a minimum, the above-mentioned parties and individuals must be screened to identify exposure to persons or entities subject to sanctions.

4.1.5 Any Other Relevant Parties

PIAS screens any other relevant parties (e.g. third party non customer payee, joint venture partners) as well as payments and other transactions initiated by the entity/associated person. ‘Payments’ include customer related payments (e.g. claims, return of investment, etc.) and PIAS related payments (e.g. supplier fees, propriety investments). The objective of screening is to identify any proposed payments to persons/entities not otherwise screened by PIAS, that may be subject to sanctions. This includes:

- Outwards payments to be made by PIAS to non-customer third-parties based in another jurisdiction
- Outwards payments to be made by PIAS to non-customer third-parties based in the same jurisdiction

4.2 What Must Be Screened

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

4.3 When Must Screening Take Place

Screening must be conducted at the initiation of the relationship and at regular intervals over the course of the ongoing relationship, when due diligence information is amended or refreshed, or the sanctions list data changes.

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

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

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

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

PIAS ensures that the timing of initial name screening via GNS complies also with relevant local sanctions legislation/regulation. For example, it is usually necessary to screen a customer before PIAS provides them with any funds or economic resources. In lower risk circumstances (e.g. where there is no transfer of funds or value from PIAS; where there are no assets to freeze; where assets within PIAS's possession cannot be withdrawn; or where confirmation/policy documents have not been issued etc.), screening within PIAS's tolerance (currently 2 days) is usually appropriate.

The tolerance for the timing and frequency of screening aligned to Group's Risk Preferences and the end-to-end timelines of clearing of alerts will be as follows.

Alert Type	**Investigation and Decision Timeline**
Sanctions Alerts (Including Prohibited Country Alerts)	Alerts investigated and a true/false decision reached within **2** business days from Alert creation.
PEP Alerts (Including PEP RCA's)	Alerts investigated and a true/false decision reached within **10** business days from Alert creation.
Other Non-Sanctions Alerts	Alerts investigated and a true/false decision reached within **30** business days from Alert creation.

4.4 Why Is Screening Conducted

Screening is conducted to identify if PIAS holds a relationship with an individual or entity subject to sanctions. This helps to ensure compliance with sanctions legislation/regulation and to identify and manage sanctions risk.

Identification of a sanctions target ('target match') must result in an assessment of the financial crime risk of that relationship and a documented decision of whether to commence, retain, reject or end the relationship and whether any sanctions obligations or restrictions are triggered as a result of the relationship.

4.5 How Must Screening Be Completed

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

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

Please refer to AML policy for more details on the various screening requirements.

4.6 Quality Checks

Quality Check (QC) reviews are carried out on 5% of all closed Alerts on a monthly basis. A list of these Alerts can be obtained by using the GNS Case Management filtering functionality and searching for:

- 'Current State: False Positive' (Sanctions, PEPs, EDD, AM and SOC)
- 'State Changed On: Selecting the appropriate date range
- State Changed By': Selecting the users against which QC is to be performed.

The QC reviewer must be conducted by someone other than the person who originally made the screening decision.

Where an alert has passed the QC; a quality control flag should be selected from the drop-down list to reflect this. Where an Alert has failed QC; relevant commentary should be added to the Alert stating why the Alert has failed QC, providing feedback to the relevant Reviewer and the Alert should be reassigned to them to update.

4.7 Prohibition Orders

MAS may, from time to time, provide circulars that include Alert Lists and Prohibition Orders. These names should already be in Dow Jones Database. As a form of assurance, screening tests are conducted to ensure the relevant names are indeed found in Dow Jones' database.

5 Group Jurisdiction Index ("JI")

Group Jurisdiction Index list ("JI") provides a blended assessment of country risk across multiple financial crime risk types.

The Group JI analyses the level of financial crime risk associated to a country by assessing various political, economic and criminal factors to produce an objective, transparent country risk rating which will be consistently applied in all PIAS' businesses. The country risk rating can be leveraged for various purposes including (but not limited to): applying a Risk Based Approach, Customer Due Diligence, Risk Assessment, Transaction Monitoring etc.

Each country in the Group JI list is rated according to the overall financial crime risk (combination of customer's nationality & domicile), with one of four ratings:

5.1 Low Risk

Countries rated "Low" are deemed to have low financial crime risk and PIAS may conduct business with these customers and they will be subjected to CDD measures and ongoing monitoring.

5.2 Medium Risk

Countries rated "Medium" are deemed to have medium financial crime risk and PIAS may conduct business with these customers, and they will be subjected to CDD measures and ongoing monitoring.

5.3 High Risk

Countries rated "high" are deemed to have high financial crime risk within the Group's Jurisdiction Index. PIAS may conduct business with customers of domicile in these countries, provided enhanced customer due diligence measures have been undertaken to ensure PIAS has made an informed risk-based decision prior to the establishment or continual of business relations.

5.4 Very High Risk

Countries rated "Very High" are deemed to have the highest financial crime risk within the Group's Jurisdiction Index. PIAS identifies and records exposure to very high risk rated countries where it conducts business in, involving with, or on behalf of, customers and counterparties based in, or customers or counterparties from, Very High Risk rated special risk countries. Potential or actual exposure to very high risk countries must be appropriately risk- assessed and approved

As a general principle, PIAS has no appetite for conducting business in, involving, with, or on behalf of, customers and counterparties based in or customers or counterparties from very high risk rated special risk countries without an appropriately approved and permissible exception.

5.5 Handling of Customers Based on Group's Jurisdiction Index

Please refer to the below table for the necessary approvals where applicable that apply to Group's Jurisdiction Index:

Nationality	Residency	Approval from CEO	Description/Conditions	ECDD Form Required
Low	Low	No	PIAS is able to conduct business with clients. *PIAS will generally prohibit business with these customers unless for exceptional cases.	No
	Medium	No		No
	High	Yes		Yes
	Very High	*Yes (For exception cases).		*Yes (For exception cases).
Medium	Low	No	PIAS may conduct business with clients. *PIAS will generally prohibit business with these customers unless for exceptional cases.	No
	Medium	No		No
	High	Yes		Yes
	Very High	*Yes (For exception cases).		*Yes (For exception cases).
High	Low	Yes	PIAS needs to make an informed risk based decision prior to the establishment or continuation of business relations with the client. *PIAS will generally prohibit business with these customers unless for exceptional cases.	Yes
	Medium	Yes		Yes
	High	Yes		Yes
	Very High	*Yes (For exception cases).		*Yes (For exception cases).

Nationality	Residency	Approval from CEO	Description/Conditions	ECDD Form Required
Very High	Low	*Yes (For exception cases).	*PIAS will generally prohibit business with these customers unless for exceptional cases.	*Yes (For exception cases)
	Medium	*Yes (For exception cases).		*Yes (For exception cases)
	High	NA	PIAS will generally prohibit business with these customers.	NA
	Very High	NA	PIAS will generally prohibit business with these customers.	NA

*** Exception Cases**

1) PIAS may consider conducting business with clients in countries rated 'Very High' if the following conditions are met:

(a) The Client is a Singaporean or Singapore PR; or
(b) Foreigner is gainfully employed in Singapore/Resides in Singapore

AND purchases
(c) CPF funded products e.g. Eldershield/or Supplement etc where the premium payments are effected via CPF funds, or
(d) Life or Health policies with cash that are reasonable and commensurate with the needs for wealth/medical protection.

AND
(e) And is not in the MAS/FATF prohibited list of countries.

Completion of ECDD form and CEO's approval are required for client on-boarding.

Risk based approach will be applied for new or existing clients with GI policies only, notwithstanding that the requirements in the above Table will not be applicable in such situations.

2) With effect from 14 October 2020, local management has approved:
   a) the onboarding of Myanmar and Pakistani customers ('Very High' risk) residing in Singapore as standard risk without the need for ECDD forms except in the following scenarios:

Nationality	Residency	Approval from CEO	Description/Conditions	ECDD Form Required

- If the Politically Exposed Person/Related Close Associate (PEP/RCA) is a beneficial owner of the customer and where the PEP/RCA originates from Myanmar or Pakistan, an ECDD form will be required.
- If the existing customer including beneficial owner becomes a PEP/RCA and they originate from Myanmar or Pakistan, an ECDD will be required.

Prohibition From Establishing Business Relations:

✓ We will **NOT** establish business relationship if the customer from Myanmar/Pakistan residing in Singapore is a PEP/RCA, where PEP/RCA status originates from Myanmar/Pakistan irrespective of country of residence.

✓ We will **NOT** establish business relationship with 'Fly in Customers' **resident** in Myanmar/Pakistan.

b) Customers from 'High' risk countries residing in Singapore do not require an ECDD form unless additional information is required for assessment.

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

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

5.5.1 Very High-Risk Countries

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

5.5.2 High Risk Countries

- for all high risk country proposals, approval from a suitably 'Designated Individual' is required (i.e. designated by PIAS' Head of Risk Management & Compliance/'Designated Individual' or equivalent)
- all high risk country proposals (approved) are to be recorded locally and included in an appropriate compliance or financial crime report to PIAS Risk Committee
- all high risk country approvals are to be notified to the Group Financial Crime Team in monthly management information reports which will be collated across the markets and included in relevant Group level reporting

5.6 Jurisdiction Index Updates & Communication

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

Changes to the JI are broadcast by the Risk & Regulatory Team via corporate announcement to all relevant contacts in PIAS. It is the responsibility of Risk & Regulatory Team to ensure that any previous versions of Group JI are replaced with the current version and that it is communicated to and shared with the relevant first and second line of defense teams.

All evidence of disseminating the updated Group Jurisdiction Index to relevant Business Units are also archived.

6 Monetary Authority of Singapore ("MAS") Sanctions

PIAS complies with financial sanction requirements set by MAS, which in turn reflects the financial sanction requirements in relation to United Nations lists of designated individuals and entities. As a member state of the United Nations (UN), Singapore is committed to implementing the UN Security Council Resolutions (UNSCRs).

MAS gives effect to targeted financial sanctions under the UNSCRs through MAS Regulations issued pursuant to Section 27A of the MAS Act 1970. The MAS Regulations apply to PIAS. Below is the list of countries that are subjected to the MAS Targeted Financial Sanctions:

- Democratic People's Republic of Korea
- Democratic Republic of the Congo
- Iran
- Libya
- Russia

- Somalia
- South Sudan
- Sudan
- Yemen

For List-based sanctions, MAS refers to UN's List from the above individual countries & The First Schedule of the Terrorism (Suppression of Financing) Act; which in turn, is reflected upon screenings done on GNS.

PIAS monitors any new sanctions legislations being updated by MAS. PIAS also updates the sanction policy whenever required in order to be in line with local and international sanctions legislations.

7 High Risk Customers

High Risk Customers are identified based on the following factors:

- High Risk Jurisdiction
- High Risk Occupation
- High Tax Risk Account
- Adverse Media Profile
- Sanctioned Individuals & Entities
- Politically Exposed Person & Relatives and Close Associates.

Please refer to PIAS's AML/CFT Policy for more information regarding High-Risk Customers.

8 Handling of Sanctioned Individual / Entity

Sanctioned individuals/entities are identified by the Risk & Regulatory Team through alerts generated via GNS system.

Customers, whose names potentially match against the names of the sanctioned individuals/entities or deemed terrorists, are flagged out as alerts in the GNS Watchlist System, where assessments are to be carried out by the Risk & Regulatory Team to ascertain if the customer is indeed a true sanctioned individual/entity

8.1 Lookback Mechanism

The trigger event for the lookback mechanism is when the Risk & Regulatory Team has ascertained the customer is indeed a true sanctioned individual/entity.

The scope of transactions that are subjected to the lookback mechanism and the period of the lookback should minimally cover all the customer's new or existing transactions such as policies and investment occurring at least 12 months preceding the date of designation.

The lookback mechanism should be initiated soon after the trigger event. The review of identified customer accounts with past transactions with sanctioned persons should be completed no later than two months after date of designation.

8.2 Internal and External Reporting of Sanctioned Individual / Entity

For confirmed sanctions matches, the following are the reporting requirements:

a) immediate reporting of confirmed sanctions target matches to RM&C
b) timely escalation (within two business days) of newly identified confirmed target matches by RM&C to MLRO
c) immediate reporting of any actual or potential breach of sanctions legislation to RM&C
d) immediate escalation of any actual breach of sanctions legislation by RM&C to MLRO
e) timely reporting (within two business days) to RM&C of other identified sanction risk exposure including for example:
    (i) relationships with a non-sanctioned entity, where one of the beneficial owners is identified as a sanctions target but the entity itself is not sanctioned
    (ii) the provision of insurance to a non-sanctioned entity (customer) for goods being shipped to a sanctioned entity/person
    (iii) relationships with a non-sanctioned person or entity, where it is identified that a relative, close associate or affiliated entity/person is a sanctions target
f) any identified local legal/regulatory reporting requirements

No external sanctions reporting of actual or suspected sanctions breaches may occur without first liaising with the MLRO 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 /MLRO, where possible in advance. This includes any application to a sanctions authority for a license or other approval.

Upon reporting, the Risk & Regulatory Team updates the register of relationships maintained with sanctioned targets. This applies to all sanctioned target matches identified, regardless of whether the sanctions are applicable in that jurisdiction or whether the relationship is held under a license from the relevant authority, or other exception.

All reporting and approvals will be archived by the Risk & Regulatory Team. The register is kept up to date.

9 Training for Employees and Representatives

The Head of Risk Management & Compliance will ensure that all employees and representatives acknowledge and commit to PIAS' approach to financial crime risks. Training is provided (as part of their induction) through the Essential Learning course, where existing and new employees, permanent or temporary contract workers, including contractors are tested yearly.

Employees are reminded that any financial crime related incident involving an employee will be considered gross misconduct and dealt with accordingly through the Group's disciplinary procedures.

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

10 Responding to Law Enforcement

PIAS documents and maintains local procedures which detail how to manage requests, enquiries or notices from law enforcement agencies and relevant regulatory/governmental authorities.

PIAS:

- ensures PIAS follows the requirement set out in local law/regulation/guidance to determine where and how to report and to identify relevant reporting templates, classification codes, submission portals;
- ensures that all requests from law enforcement and relevant regulatory/governmental authorities are fully complied with, in a timely manner and in compliance with local data protection requirements;
- incorporates any rules and regulations around 'tipping off' to ensure that the subject of concern is not made aware that such a request has been made;
- identifies and documents who will be responsible for responding to such requests and ensure that in all cases the relevant person is consulted before releasing any information;
- maintains a log to record all requests received from and all information provided to law enforcement agencies and relevant regulatory/government authorities;
- If following the receipt of an order/enquiry/request or during the collation/review of information, a suspicion of financial crime arises, the local relevant internal and external reporting procedures are followed (Please refer to AML/CFT policy for more information on reporting);
- the receipt of an order/enquiry/request does not absolve individuals or PIAS of existing responsibilities under financial crime legislation, for example any obligation to report suspected money laundering. Further advice may be sought from the Risk & Regulatory Team.

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

12 Record Keeping

PIAS maintains full audit trails of business activities to demonstrate financial crime risks management and has procedures in place to manage financial crime risks including those relating to sanctions, through documentary evidence.

In addition, the retrieval of documents, records and information is a key component of being able to provide MI, develop intelligence and respond to law enforcement, audit or regulatory scrutiny.

12.1 Record Retention & Retrieval

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

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

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

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

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

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

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

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

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

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

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