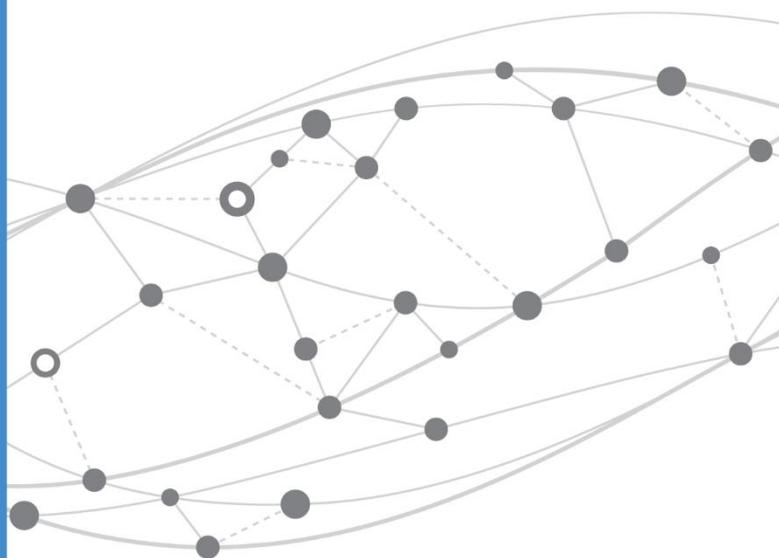
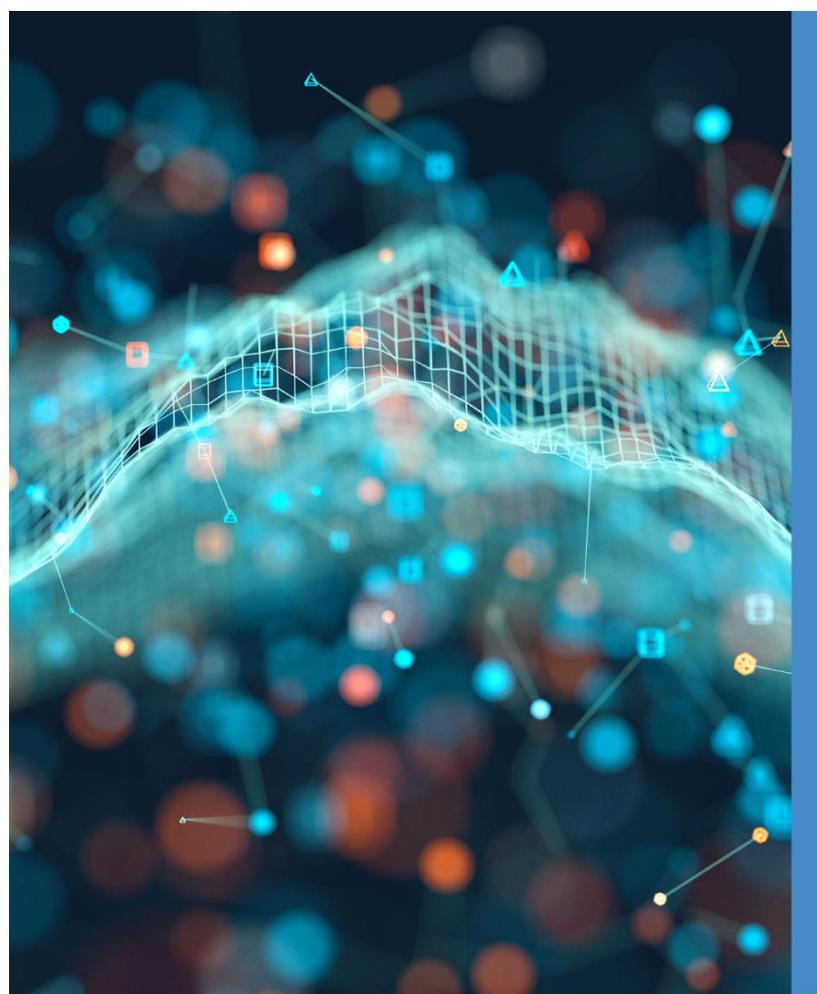


GAM GLOBAL AML & FINANCIAL CRIME PREVENTION POLICY



GAM Global AML and Financial Crime Prevention Policy

As of 22/05/2021

GAM Global AML & Financial Crime Prevention Policy

Applies to: GAM Holding AG and each of its subsidiary companies, partnerships and branch offices (collectively the “Group” or “Global” and each a Group Company”)

Effective from: 22nd May 2021

Policy Owner: Global Head of Financial Crime Prevention & MLRO

Document Management

Policy Owner	Version Effective Date	Review Frequency	Next Review Date	Published
Global Head of Financial Crime Prevention & MLRO	V1.0 March 2020	Annual	April 2021	Approved by GAM PMC & SLT 25/03/2020
Global Head of Financial Crime Prevention & MLRO	V1.1 May 2021	Annual review with feedback from Lux & Swiss	June 2022	Approved by Paul Simmons Global Head of Financial Crime

Index

1. Purpose	3
2. Scope	3
3. AML and Financial Crime Legislation	3
4. Governance & Organisation	4
5. Policy Principles	4
6. Due Diligence	6
7. Sanctions Screening	6
8. Politically Exposed Persons (PEPs)	7
9. Adverse Information Screening	7
10. Third Party Payments	8
11. Tax Evasion	8
12. Fraud	8
13. Suspicious Activity Reporting (SAR) & Investigation	8
14. Training	9
15. Record Keeping & Retention	9
16. Exceptions to this Policy	9
17. Information Access	9
Appendix 1 – PEP Categories	10
Appendix 2 – Definitions	12
Appendix 3 – GAM Group AML Jurisdictional Heatmap	13

1. Purpose

The purpose of this GAM Global AML and Financial Crime Prevention Policy which includes Money Laundering, Terrorist Financing, Sanctions Screening and Politically Exposed Persons (this 'Policy') is to establish the minimum standards to be followed by GAM Holding AG and all its related group companies ("Group") in order to comply with applicable legal and regulatory requirements and to mitigate its financial crime risk exposure. Furthermore, this policy shall ensure that global standards of the Financial Action Task Force (FATF) and FINMA's basic AML principles are met and that local rules do not contradict these basic principles. Each Group Company shall define its local AML and financial crime prevention requirements in a separate local policy that at least meets these standards.

The Group recognises the need to have in place appropriate and proportionate risk based policies, procedures, systems and other controls to protect its clients (including investors in GAM funds where applicable), group companies, employees and other stakeholders by deterring, detecting and preventing those who would seek to use the Group or a GAM fund to facilitate any form of money laundering or financial crime.

Failing to manage financial crime risks effectively undermines the integrity of the financial system and society. Furthermore, failure to comply with AML or financial crime prevention regulations can be a criminal offence, and failing to identify, manage and monitor financial crime risks adequately could expose the Group's clients to loss and the Group and its employees to potential prosecution and penalties and/or regulatory penalties and censure, damage client and business partner confidence in the Group and result in reputational harm.

2. Scope

This Policy applies to all employees (including contractors), each Group Company (including branches) and its board of directors, Group Board and GAM fund.

This policy covers the following financial crime areas:

- Money Laundering
- Terrorist financing
- Sanctions Screening
- Politically Exposed Persons
- Suspicious Activity Reporting
- Tax Evasion
- Training
- Record Keeping

This policy excludes the following areas:

- Anti-bribery and corruption
- Market Abuse

3. AML and Financial Crime Legislation

This Policy has been influenced by global financial crime standards as set out in the 40 FATF Recommendations for preventing money laundering, terrorist financing and financial crime, the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA) of Switzerland, and the EU Money Laundering Directives.

4. Governance and Oversight

The GAM Holding AG Board designates responsibility for financial crime related matters to the Global Head of Financial Crime Prevention.

GAM Group Board's will:

- Encourage and maintain effective systems and controls to prevent money laundering and financial crime.
- Designate each local MLRO (or compliance officer with AML responsibility) to have the responsibility in their applicable jurisdiction for the oversight of financial crime risk and any related reporting or filings as may be required in the applicable jurisdiction.

Senior Management (GAM Group and GAM Group companies):

Senior Management have a role in the Group's prevention of financial crime, including assisting in the management of the Group's exposure to financial crime risk in accordance with this policy, and ensuring appropriate support to their local MLRO's in ensuring effective systems and controls are in place to prevent money laundering and financial crime.

The Global Head of Financial Crime Prevention:

The Global Head of Financial Crime Prevention is responsible for:

- Establishing, owning and maintaining the Group AML and Financial Crime Prevention Policy.
- Providing guidance to and oversight of each local business unit in terms of AML and financial crime prevention.
- Being the escalation point for high-risk clients, sanctions and PEPs advice and guidance, and where appropriate approval.

Local MLROs:

Each MLRO has a role in the Group's prevention of financial crime, including to discharge such duties of an MLRO as prescribed by relevant regulation and shall:

- Act as the focal point for all activity within the applicable Group Company relating to Financial Crime Prevention.
- Be an approver for all high-risk clients and PEPs relationships.

Employees

Employees (including all contractors working for GAM) are required to comply with this Policy, including all Group and relevant local policies, procedures, guidance and other controls; to undertake applicable mandatory training and to report any suspicion of financial crime that may arise in the course of their employment or contract to the applicable MLRO.

5. GAM Global AML & Financial Crime Prevention Principles

GAM Group is committed to combating financial crime and ensuring that its products are not misused for the purpose of money laundering, terrorism financing or fraud events. GAM always operates in adherence with applicable laws and regulations regarding anti-money laundering, sanctions and anti-bribery and corruption. GAM has no appetite for clients who fail to comply with our financial crime policies or procedures.

Each GAM Group Company must adhere to the following principles in terms of preventing money laundering (AML), terrorist financing (CTF) and financial crime:

1. Ensure there are systems and controls in place to mitigate against money laundering, terrorist financing and financial crime and that such measures remain effective.
2. Appoint an MLRO (or compliance officer with AML responsibility) for each Group Company to ensure AML and CTF monitoring and controls are implemented in line with the local regulations and this Policy.
3. Apply a risk-based approach to client onboarding due diligence (Low-Standard/ Medium / High), these will be reviewed annually for high risk, every 3 years for medium and every 5 years for low-standard.
4. Onboard new business using a risk-based approach only when the Contracting Party (individual or legal Company) is duly identified, the company is satisfactorily verified, and the Beneficial Ownership or Controlling Person is properly established in line with local regulatory requirements.
5. Ensure due diligence is maintained and kept up to date through regular periodic reviews.
6. Ensure that a risk-based approach is utilised for the identification and verification of UBOs of corporate entities, foundations and trusts and other structures.
7. Ensure regular sanctions and PEPs screening is maintained and matches are dealt with appropriately.
8. All PEPs to be approved by BU heads, local MLRO's and the Global Head of Financial Crime Prevention.
9. Implement controls for the reporting of suspicions regarding money laundering, terrorist financing and tax evasion activities.
10. Ensure employees are aware of their obligations and receive adequate financial crime awareness training.
11. Report suspicious activity promptly to the MLRO, who will determine whether the activity is suspicious from a financial crime perspective and report to the relevant law enforcement authority.
12. Maintain policies, procedures, and processes to implement the above requirements.
13. Support the local regulators in maintaining the integrity and transparency of the financial markets.
14. Make sure regular management information is created and shared with key stakeholders as a minimum. This should include an annual MLRO report or equivalent to the relevant GAM Board.

Prohibited Activity outside of GAM Group companies Risk Appetite:

- ❖ Do not establish business relationships with individuals and companies identified to be associated with any financial crime or illegal activities.
- ❖ Do not accept any assets which you know or must assume to be the result of a crime.
- ❖ Do not establish business relationships where the Beneficial Owners or Controlling Persons are not properly established.
- ❖ Do not establish business relationships with corporates who are permitted to issue bearer shares.
- ❖ Do not establish business relationships with shell banks and companies.
- ❖ Do not establish business relationships with companies based or operating in a sanctioned regime.
- ❖ Do not establish business relationships with politically exposed persons (PEPs) linked to bribery and corruption.

Group-wide Risk Assessment

The Group has standardized reporting at least once a year with sufficient quantitative and qualitative information from the group companies so that it can reliably assess its AML, financial crime and resulting reputational risk on a consolidated basis.

The Group companies shall take a risk-based approach to the acceptance and continuation of the globally most significant relationships and transactions as well as of other significant changes in legal and reputational risks. In particular, if these risks relate to significant assets connected with high risk politically exposed persons or companies outside of GAM Group risk appetite. These will be escalated to the Global Head of Financial Crime if appropriate and will be reported to the GAM Holding AG Board if representing a significant risk. The Group's AML or compliance function shall on a risk-based approach carry out regular reviews of risk-based internal controls, including spot checks on individual business relationships and on site at branch offices and group companies.

6. Due Diligence

All prospective clients and counterparties must be risk assessed by applying a risk-based approach to ensure the appropriate level of due diligence is applied.

GAM Group has systems and controls in place to ensure CDD is performed on its clients and counterparties to verify identity and validate that there are no legal or financial crime risk appetite reasons to decline entering into such a business relationship, and to also acquire appropriate and meaningful information to assist monitoring of the business relationship.

There are three levels of due diligence that can be applied to clients and counterparties:

❖ **Standard due diligence (Low Risk)**

Standard due diligence will be applied for relationships where clients/counterparties are considered to represent a low risk. This should include a minimum CDD/KYC on those who own or control 25 % of the entity and this relationship should be reviewed on a 5-yearly basis. For those entities that are listed or regulated and represent a lower money laundering risk, the Group takes a risk-based approach on the identification and verification of owners and controllers.

❖ **Regular due diligence (Medium Risk)**

Regular due diligence will be applied for relationships where clients/counterparties are considered to represent medium risk. This should include a minimum CDD/KYC on those who own or control 25 % of the entity and this relationship should be reviewed on a 3-yearly basis.

❖ **Enhanced due diligence (High risk)**

Enhanced due diligence will be applied on a risk-sensitive basis in any situation where the client or counterparty presents a higher risk of being exposed to financial crime risks (this includes but is not limited to PEP ownership and control), this should include a minimum CDD/KYC on those who own or control 25 % of the entity. All high-risk clients should be approved by the local MLRO, the Business unit head, and if appropriate escalate to the Global Head of Financial Crime Prevention.

Ultimate Beneficial Ownership (UBO)

Ultimate beneficial ownership confirmation is obtained from independent and reliable sources.

Regulated & Listed Entities:

A risk-based approach is used for the identification and verification (ID+V) of the UBOs/controlling persons/directors of regulated entities. For low and medium-risk regulated entities, if having determined that there are no parties that own more than 25% of shares then the controlling directors must be identified and where appropriate verified.

For high-risk regulated entities, if having determined that there are no parties that own more than 25% of shares then the controlling directors must be identified, and verification documentation must be obtained.

For Unregulated Entities:

For unregulated entities of all risk categories, identification and verification must be obtained for all shareholders owning more than 25% of shares. In addition, identification and verification must be obtained for at least two controlling directors of low and medium-risk unregulated entities and at least four controlling directors of high-risk entities.

7. Sanctions:

1. GAM Group companies will not knowingly engage in a business relationship with any individuals/companies/counterparties that are listed on the following sanctions lists – HM Treasury (UK),

EU Sanctions lists, UN Sanctions lists and Office of Foreign Assets and Controls list (OFAC-USA) and other sanctions lists as deemed necessary according to local laws (i.e. the Seco (Swiss State Secretariat for Economic Affairs)).

2. GAM Group companies will screen all individuals/companies/counterparties against sanctions lists prior to commencing their business relationship with GAM Group and thereafter on a regular basis throughout the life cycle of their relationship with GAM.
3. GAM Group companies will (i) reject any business relationships that are identified as a sanctions match or exit any existing relationships and (ii) initiate any reporting necessary due to local requirements. Any sanctions matches identified will lead to the immediate freezing of the company/individuals account and will be reported to the local law enforcement authority.

8. Politically Exposed Persons (PEP's):

1. GAM Group companies take a risk-based approach concerning the acceptance of a business relationship with politically exposed persons or companies, this will take into consideration the risk they pose to the brand and reputation of GAM in terms of financial crime and bribery and corruption risks.
2. All PEPs identified will be accepted on a risk-based approach taking into consideration the significance of their level of political exposure, the jurisdiction where they are politically exposed, their conduct and behaviour from a bribery and corruption, financial crime or ethical perspective.
3. GAM Group companies will screen all individuals/companies/counterparties against PEPs lists prior to commencing their business relationship with GAM Group and thereafter on a regular basis throughout the life cycle of their relationship with GAM.
4. All PEP relationships to be approved by local MLRO's and local relationship business heads and the Global Head of Financial Crime Prevention.
5. All PEP relationships will be subject to enhanced due diligence which will include source of funds and wealth information as well as annual reviews to determine their suitability from a risk appetite perspective in continuing the relationships.
6. All PEPs will be considered as politically exposed persons for a minimum of one year after they have left their office, however, local MLRO's will apply a risk-based approach to this timing depending on the nature and profile of the PEP and the respective local requirements.
7. PEPs will only be declassified once approved by the local AML Officer/MLRO. A review of the PEP will be conducted and an assessment will be made using a risk-based decision as to the levels of risk the PEP role(s) pose to the GAM business.

9. Adverse Information Screening:

1. Adverse media or negative news is any kind of unfavourable information found across a wide variety of news sources. There are specific reputational and regulatory risks associated with conducting business with persons or companies having an adverse media profile.
2. Adverse media checks can reveal involvement with money laundering, fraud, tax evasion, organised crime, terrorism and bribery and corruption. These factors could pose a serious threat to firms' reputations and

can lead to legal repercussions. Any clients associated with this activity will be fully investigated to determine whether they are within GAM's risk appetite.

10. Third Party Payments:

GAM Group companies make third party payments on a risk-based approach due to the inherent financial crime risks of this type of transaction. These should only be allowed by local MLRO's/Finance Managers and Risk units if there is a clear business rationale for it and the risks of fraud, money laundering and tax evasion between the accounts have been clearly discounted.

11. Tax Evasion:

GAM Group companies will not knowingly assist a client in evading paying their taxes. Any incidents of tax evasion will be thoroughly investigated by local MLRO's to determine if the activity is tax evasion (criminal offence) or tax avoidance. Any suspicions about tax evasion will be escalated to the Global Head of Financial Crime.

12. Fraud:

GAM Group is committed to preventing, detecting, and reporting fraud, and in co-operating with other organisations to reduce opportunities for fraud. GAM Investments is committed to ensuring that clients, employees and vendors are protected from fraudulent activities. Fraud is defined as the deliberate use of deception or dishonesty to disadvantage or cause loss (usually financial) to another person or party. Fraud is an issue that companies may face regardless of size, industry or country. GAM's fraud risk is managed by:

- ❖ defining, setting and maintaining effective control procedures to identify and deter fraud;
- ❖ investigating all incidences of actual, attempted or suspected fraud, and all instances of major control breakdown;
- ❖ encouraging staff to be vigilant and raising fraud awareness through regular training;
- ❖ ensuring key controls are complied with;
- ❖ providing staff with effective confidential reporting mechanisms and encouraging their use;
- ❖ taking action against individuals and organisations perpetrating fraud against GAM; and
- ❖ co-operating with the police and other appropriate authorities in the investigation and prosecution of those suspected of fraud.

13. Suspicious Activity Reporting (SAR) and Investigation:

1. GAM Group companies will ensure all incidents of concern or suspicion(s) from a financial crime perspective in terms of money laundering, terrorist financing, sanctions breaches, fraud, tax evasion, market abuse or bribery and corruption will be thoroughly investigated by the local MLRO and that the appropriate reports are immediately made to law enforcement (or other appropriate authority(s)) and shared with other potentially impacted GAM Group entities.
2. GAM Group companies delegate responsibility for SAR investigation and reporting to the relevant local MLRO's, any significant issues should be escalated to the Global Head of Financial Crime Prevention for advice and guidance.
3. Suspicious activity is investigated primarily through the suspicious incident reports (SIRs) process. Internal investigations are conducted to determine the profiles of relevant parties, the relevant behaviours and any funds that may have been lost. All SIR investigations are clearly documented to maintain a transparent audit trail. If there is a reasonable belief that criminal activity has taken place, then the local MLRO will raise a suspicious activity report (SAR) to law enforcement.

-
- All SAR investigations will be clearly documented to maintain a clear audit trail of suspicions to ensure an accurate record of grounds of suspicion, investigation(s) conducted and the decision taken by the local MLRO whether or not to report the SAR to law enforcement/FIU or regulator (or other appropriate authority(s)). Any decision taken not to make a report will be clearly documented for audit purposes. These records will be held indefinitely in case they are requested at a future date by government agencies or the regulator (or other appropriate authority(s)).

14. Training:

Regulatory training shall be rolled out to all employees on an annual basis and cover key AML and financial crime risk areas, this includes all employees including temporary contractors. All new starters will complete their training within 35 days of joining GAM.

15. Record Keeping and Retention:

- GAM Group companies will ensure they comply with regulatory requirements and assist law enforcement agencies (or other appropriate authority(s)) with any requests for information.
- All data obtained for client and counterparty identification, AML purposes and measures must be documented, securely stored in an accessible manner and kept for a minimum of 5 years after the end of the business relationship or for such longer period required under applicable local laws.

16. Exceptions to this Policy:

Exceptions to this policy can be requested from the Global Head of Financial Crime Prevention. In considering whether or not to grant such an exception, the Global Head of Financial Crime shall have regard to all the relevant circumstances, including the Group's risk appetite for Financial Crime risks.

17. Information Access:

GAM grants access to information on business relationships in all Group companies to the internal supervisory bodies, the audit firm of the Group and the responsible persons such as the Compliance function, MLRO and the Global Head of Financial Crime Prevention on request and without delay, which is required for the global monitoring of legal and reputational risks.

Appendix 1- PEP Categories

Types:

- ❖ Individuals (foreign or domestic)
- ❖ Relatives and Close Associates
- ❖ Companies (corporates or trusts) owned or controlled by PEPs
- ❖ State Owned Entities (SOE's) – Majority 50% owned by the State

Area of PEP Exposure

PEP Exposure	Definition of Role
STATE – Heads of state, heads of government, ministers and deputy or assistant ministers	<ul style="list-style-type: none"> ❖ King/Queen ❖ Prime Minister ❖ President ❖ Emperor ❖ Cabinet Minister ❖ Minister (Significant function)
PARLIAMENT – Members of parliament or similar legislative bodies	<ul style="list-style-type: none"> ❖ Members of National Assembly ❖ Member of administration ❖ Member of house of lords ❖ Member of local Assembly
POLITICAL PARTIES – Members of the governing bodies	<ul style="list-style-type: none"> ❖ Political party leaders /Deputy Leaders ❖ Privy Council ❖ Members of European Parliament (MEPs)
JUDICIAL – Members of supreme courts, of constitutional courts or of any judicial body	<ul style="list-style-type: none"> ❖ Supreme Court judges ❖ European Court of Justice (ECJ) ❖ European Court of Human Rights (ECHR) ❖ International Court of Justice ❖ Court of Appeal Judges
BANKING AND AUDITING – Member of courts of auditors or of the boards of central banks	<ul style="list-style-type: none"> ❖ Central Bank Governor ❖ Central Bank Board ❖ Court of auditors/directors ❖ European Central Bank ❖ European Banking Authority
DIPLOMATIC AND MILITARY – Ambassadors, charge d'affairs, and high ranking officers in the armed forces.	<ul style="list-style-type: none"> ❖ Ambassador ❖ Charge D'Affair ❖ Permanent Secretary ❖ Deputy Permanent Secretary ❖ Admiral Vice Admiral ❖ Lieutenant General ❖ Air Marshal
STATE OWNED ENTERPRISE – Members of the administrative, management or supervisory bodies of state owned enterprise.	<ul style="list-style-type: none"> ❖ Chairman ❖ Board Member ❖ CEO ❖ Secretary General
SIGNIFICANT INTERNATIONAL ORGANISATIONS – Directors, deputy directors and members of the board or equivalent functions of an international organisation.	<ul style="list-style-type: none"> ❖ Chairman ❖ Board member or equivalent ❖ Directors ❖ Deputy Directors ❖ CEO ❖ Secretary General

PEP – Relative and Close Associates

1. Relative of PEP

Relatives – Potential Area of PEP Exposure
<ul style="list-style-type: none"> ❖ Spouse ❖ Civil Partner ❖ Brother/Sister ❖ Child ❖ Child’s spouse or Civil Partner ❖ Parents

2. Close Associate of PEP

Close Associates – Potential Area of PEP Exposure
<ul style="list-style-type: none"> ❖ Significant influence employees ❖ Directors (Executive and Non-Executive) ❖ Significant influence client ❖ Personal Banker /Wealth Manager/Accountant ❖ Legal Counsel ❖ Close Business Associates ❖ Power of Attorney ❖ Joint Beneficial Owner of a legal Company, trust or arrangement ❖ Advisors – financial/lawyer or tax

Appendix 2 – Definitions:

FCPT	Financial Crime Prevention Team
MLRO	Money Laundering Reporting Officer
SAR	Suspicious Activity Report
HMT	Her Majesty's Treasury
PEP	Politically Exposed Persons
AML	Anti-Money Laundering
CDD	Client/Counterparty Due Diligence
CRA	Client/Counterparty Risk Assessment
CTF	Combating Terrorist Financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Units
KYC	Know Your Client
OFAC	US Office of Foreign Assets Control
Controlling Person/ Directors	the natural person of an operating legal Company who ultimately controls the legal Company in that they directly or indirectly, alone or in concert with third parties, hold a significant percentage of 25% or less (specified according to local laws) of the capital or voting rights in the legal Company or otherwise control it (i.e. directors).
Beneficial Owner	means the individual person that ultimately has the ownership of the assets.

Appendix 3 – GAM Group AML Jurisdictional Heatmap

<u>Low Risk Countries</u>					
Australia	Denmark	Hong Kong	Luxembourg	Singapore	United Kingdom
Austria	Estonia	Iceland	Netherlands	Spain	United States
Belgium	Finland	Ireland	New Zealand	Sweden	Uruguay
Canada	France	Italy	Norway	Switzerland	
Chile	Germany	Japan	Portugal	Taiwan	

<u>Medium Risk Countries</u>					
Andorra	Czech Republic	Hungary	Lithuania	Qatar	St. Lucia
Brazil	Dominica	Isle of Man	Macedonia	Romania	St. Vincent & the Grenadines
Bulgaria	Egypt	Israel	Monaco	Slovakia	United Arab Emirates
Costa Rica	Greece	Jersey	Montenegro	Slovenia	
Croatia	Grenada	Latvia	Oman	South Africa	
Cyprus	Guernsey	Liechtenstein	Poland	South Korea	

<u>High Risk Countries</u>					
Afghanistan	Aland Islands	Albania	Algeria	American Samoa	Angola
Anguilla	Antarctica	Antiqua and Barbuda	Argentina	Armenia	Aruba
Azerbaijan	Bahamas	Bahrain	Bangladesh	Barbados	Belarus
Belize	Benin	Bermuda	Bhutan	Bolivia	Bonaire St. Eus & Saba
Bosnia & Herzegovina	Botswana	Bouvet Island	British Indian Ocean Territory	British Virgin Islands	Brunei Darussalam

Burkina Faso	Burundi	Cambodia	Cameroon	Cape Verde	Cayman Islands
Central African Republic	Chad	China	Christmas Islands	Cocos Islands	Colombia
Comoros	Congo (Brazzaville)	Congo Dem.Rep	Cook Islands	Cote D'Ivoire	Curacao
Djibouti	Dominican Republic	Ecuador	El Salvador	Equatorial Guinea	Eritrea
Ethiopia	Falkland Islands	Faroe Islands	Fiji	French Guiana	French Polynesia
French Southern Territories	Gabon	Gambia	Georgia	Ghana	Gibraltar
Greenland	Guadeloupe	Guam	Guatemala	Guinea	Guinea-Bissau
Guyana	Haiti	Heard Islands & McDonald Islands	Holy See (Vatican City State)	Honduras	India
Indonesia	Iraq	Jamaica	Jordan	Kazakhstan	Kenya
Kiribati	Kosovo	Kuwait	Kyrgyzstan	Lao People's Dem. Rep.	Laos
Lebanon	Lesotho	Liberia	Libya	Macau	Madagascar
Malawi	Malaysia	Maldives	Mali	Malta	Marshall Islands
Martinique	Mauritania	Mauritius	Mayotte	Mexico	Micronesia
Moldova	Mongolia	Montserrat	Morocco	Mozambique	Myanmar
Namibia	Nauru	Nepal	Netherlands Antilles	New Caledonia	Nicaragua
Niger	Nigeria	Niue	Norfolk Island	Northern Mariana Islands	Pakistan
Palau	Palestinian Occupied Territory	Panama	Papua New Guinea	Paraguay	Peru
Philippines	Pitcairn Islands	Puerto Rico	Reunion	Russia (Incl. Crimea & Sevastopol)	Rwanda

Saint Barthélemy	St. Helena, Ascension & Tristan da Cunha	Saint Martin (Dutch Part)	Saint Martin (French Part)	Saint Pierre & Miquelon	Samoa
San Marino	Sao Tome & Principe	Saudi Arabia	Senegal	Serbia	Seychelles
Sierra Leone	Solomon Islands	Somalia	South Georgia & the South Sandwich Islands	Sri Lanka	St Kitts & Nevis
Sudan	Suriname	Svalbard & Jan Mayen	Swaziland	Tajikistan	Tanzania
Thailand	Timor-Leste	Togo	Tokelau	Tonga	Trinidad & Tobago
Tunisia	Turkey	Turkmenistan	Turks & Caicos	Tuvalu	Uganda
Ukraine	United States Minor Outlying Islands	Uzbekistan	Vanuatu	Venezuela	Vietnam
Virgin Islands, U.S.	Wallis & Futana	Western Sahara	Yemen	Zambia	Zimbabwe

Prohibited Countries

Cuba	Iran	North Korea	South Sudan	Syria
------	------	-------------	-------------	-------