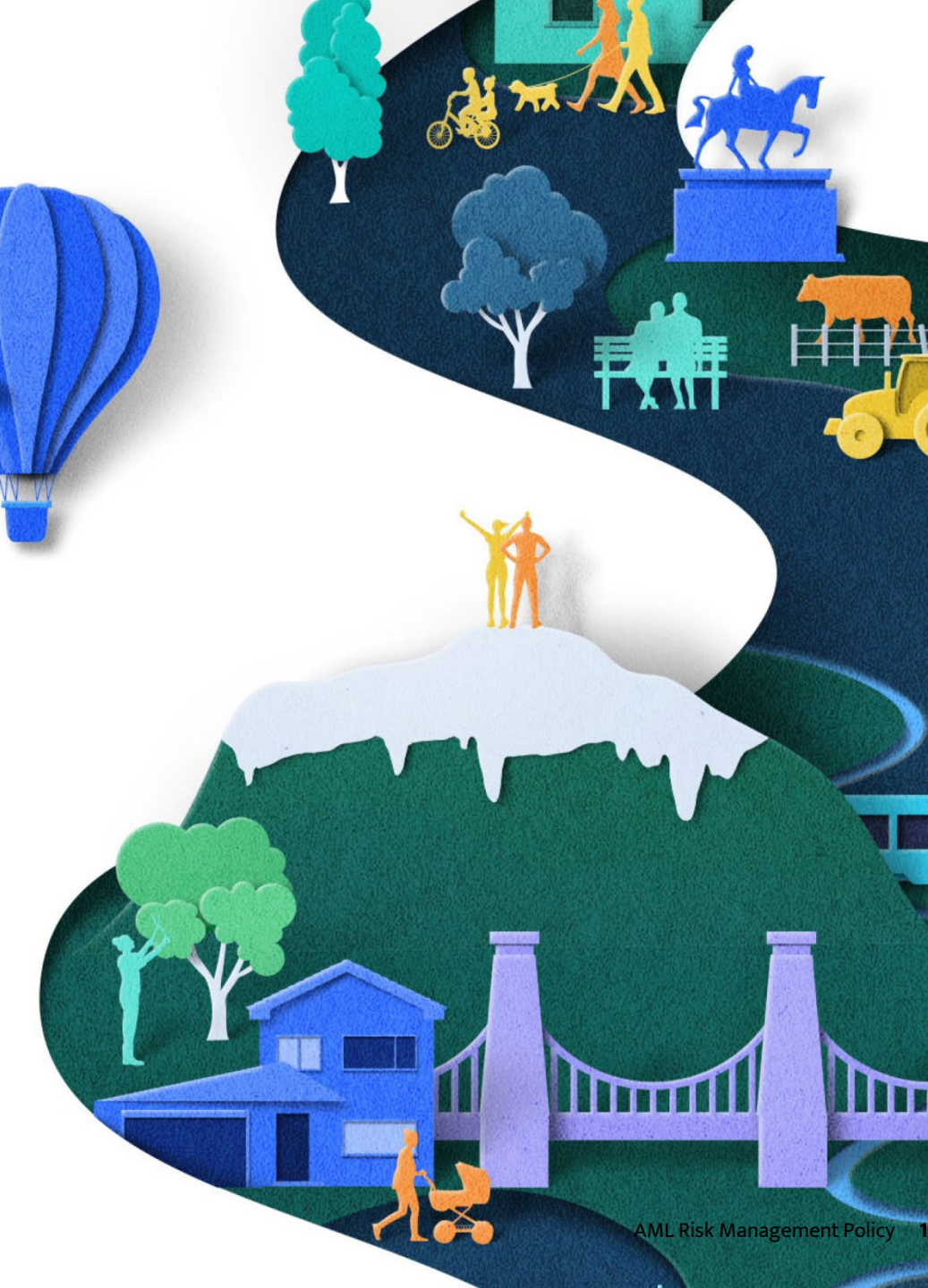
Anti-Money Laundering, Terrorist Financing, Facilitation of Tax Evasion & Sanctions Risk Management Policy



Policy Owner	Money Laundering Reporting Officer
Approving Body	Board Risk Committee
Date Approved	28th November 2023
Next Review Date	May 2024
Review Frequency	Annually
Document Management	V0.1

Table of Contents

Definition, purpose & policy

How do we define money laundering, terrorist financing, facilitation of tax evasion & sanctions Risk?	Non-compliance with legislative and regulatory Money Laundering, Counter Financing of Terrorism, or Sanctions requirements.
What is the purpose of this Policy?	The Society's Anti-Money Laundering, Terrorist Financing, Facilitation of Tax Evasion, and Sanctions Risk Management Policy is produced in accordance with the requirements of the Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017, Proceeds of Crime Act 2002, Terrorism Act 2000 (and Anti-Terrorism Crime and Security Act 2001), Counter Terrorism Act 2008, Immigration Act 2016, Sanctions and Anti-Money Laundering Act 2018, and Criminal Finances Act 2017. The purpose of the Policy is to communicate the Society's approach to managing the stated risks, and the responsibilities and arrangements in force for carrying out the Policy.

What is our Policy?

Risk Appetite
The Society has a low appetite for Financial Crime risk (and no appetite for money laundering, terrorist financing, facilitation of tax evasion, and sanctions risk), meaning the Society will normally accept: 1) green residual risks; ii) amber risks with approved action plans; and iii) a moderate cumulative impact of events across a 12 month period.

Policy Objectives
- Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal conduct, thereby avoiding prosecution, conviction and the confiscation of the criminal funds.
- Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.
- Facilitating tax evasion is the involvement in making plans to evade taxes on assets.
- Financial sanctions are restrictions put in place by the UN or UK to achieve a specific foreign policy or national security objective. They can limit the provision of certain financial services and restrict access to financial markets, funds and economic resources.

The Society's Board requires that the risk of money laundering, terrorist financing and the facilitation of tax evasion affecting the accounts, records, money or other assets of the Society and its members, whether by colleagues, members, or third parties, is kept to as low a level as is reasonably achievable.

The Society has a low risk business model. The Society operates only in the UK and offers mortgages and savings accounts to private individuals (with a small back-book of non-private accounts). Controls are focused on minimising the risk of the Society's accounts being used for the purpose of money laundering and terrorist financing. This includes the identification and proactive management of higher risk customers, including those that may be subject to financial sanctions or are categorised as politically exposed persons (PEPs) or otherwise present a higher risk to the Society due to their customer profile e.g. criminality, high risk jurisdiction, or suspicious activity.

The objectives of the Policy are:
- To encourage compliance with all laws and regulations relevant to sanctions, money laundering and terrorist financing (as stated above).
- To prevent, detect and limit the Society's products and services from being exploited by criminals and terrorists for money laundering and terrorist financing purposes.
- To prevent, detect and limit the involvement of those acting on the Society's behalf in the criminal facilitation of tax evasion.

This Policy is reviewed by the Board Risk Committee on an annual basis or when warranted due to changes to the business or external factors.

Reliance Upon and Boundaries with Other Risk Categories
In determining appropriate content for this Policy, activities which may give rise to Money Laundering risk were considered. Where required, boundaries with other Risk Categories have been determined: Fraud; People; Third Party; Anti-Bribery and Corruption; Transaction Processing, and Data Protection.

Other standards and processes are relevant in the Society's management of Anti-Money Laundering risk including: Anti-Money Laundering Handbook; Whistleblowing policy; ID Guidance; and Treasury Risk Management Policy.

Return to Table of Contents

Scope, compliance & policy breaches

Who does this Policy apply to?

This Policy applies to all employees, contingent workers, business areas and companies within the Society, regardless of working location.

It is the responsibility of all employees and contingent workers to maintain awareness of, and comply with this Policy and any associated standards, guidelines or procedures.

How is compliance with the Policy monitored, overseen and assured?

The Society adopts a Three Lines of Defence (3LoD) approach to monitoring, oversight and assurance.

Compliance with the Policy is monitored by the AML team under the guidance of the Head of Conduct Risk Oversight and Compliance, who is also the Money Laundering Reporting Officer (MLRO), using the following mechanisms:

- Review and challenge of first line RCSA;
- Review and challenge of first line controls assurance;
- Review of risk events reported via the Society's risk management system;
- Monitoring and review of Risk Acceptances and Exceptions to Policy; and
- Monitoring completion of risk mitigation actions.

Additional independent assurance will be gained from Operational Risk oversight, Compliance inspections and reviews, and Internal Audits.

How should breaches or exceptions to this Policy be recorded and escalated?

Policy Breaches
All policy breaches should be recorded in the Society's risk management system. If the breach has caused, or has the potential to cause a 'Moderate' or above impact (as assessed against the Society's Risk Impact Matrix), it must be notified to the MLRO, the Head of Financial Crime, and the Operational Risk team within 24 hours after identification.

Exceptions to Policy
No deviations to the policy are permitted unless an Exception to Policy has been formally agreed with the MLRO. All requests for Exceptions to Policy must be requested using the Society's Risk Acceptance Request Form and forwarded to the Operational Risk Team.

Return to Table of Contents

Roles & Responsibilities

Board

Responsible for the review of the annual report of the Money Laundering Reporting Officer.

Board Risk Committee

Responsible for the approval of the Anti-Money Laundering Risk Management Policy.

Operational Risk Committee (ORC)

Responsible for the review of the Anti-Money Laundering Risk Management Policy, the annual report of the Money Laundering Reporting Officer, and the Financial Crime risk category dashboard including key risk indicators relating to Anti-Money Laundering risks.

All colleagues

Every colleague shall remain alert for the possibility of money laundering and terrorist financing, and shall report any and every suspicion for which they believe there are reasonable grounds, following the Society's procedure.

The expectation placed on each individual colleague in responding to possible suspicions shall be appropriate to their position in the Society. No-one is expected to have a greater knowledge and understanding of customers' affairs than is appropriate to their role.

All customer facing colleagues (retail and wholesale customers) and AML team

- Verify the identity of all customers according to the ID Guidance, ensuring that procedures reflect customer risk characteristics. The Society will check that customers are not the subject of sanctions or other statutory measures prohibiting the Society from providing its services.
- Obtain information enabling it to assess the purpose and intended nature of every customer's relationship with the Society. This Know Your Customer information will enable the Society to maintain its assessment of the on-going money laundering and terrorist financing risk, and identify changes or anomalies in the customer's arrangements that could indicate money laundering or terrorist financing. Further, the Society will not offer its services if a satisfactory understanding of the nature and purpose of the customer's business with us cannot be achieved.
- Monitor customers' instructions and transactions to ensure consistency with those anticipated and with the customer risk profile. Instructions and transactions will be monitored to ensure that possible grounds to suspect money laundering, terrorist financing or facilitation of tax evasion will be noticed and scrutinised, and changes requiring a re-assessment of risk will be acted upon.
- Establish and maintain systems to keep records of enquiries made and information obtained while exercising customer due diligence for anti-money laundering purposes, and to ensure that these records are retrievable as required for legal and regulatory stipulations. These records will include but not be limited to details recorded for accounting and business development purposes.

Procurement

Establish and maintain systems to keep records of enquiries made and information obtained while exercising supplier due diligence for anti-money laundering purposes, and to ensure that these records are retrievable as required for legal and regulatory stipulations.

People Services

Recruitment of all new colleagues will include assessment as described in section 21(2) of the Money Laundering Regulations. Screening for fraud and money laundering risk will take place prior to appointment. Periodic screening will also take place for relevant employees (as defined in section 21(2b)) during the course of the appointment.

AML Team

Investigates and assesses individual cases reported to it or identified through transactions monitoring systems, and liaises with law enforcement agencies as appropriate.

Return to Table of Contents

Roles & Responsibilities (cont.)

AML Management including MLRO

- Prepare and present an annual MLRO Report to the Board.
- Maintain a business wide AML risk assessment to ensure that the Society is well placed to meet its legal and regulatory obligations in relation to AML, including ongoing compliance with the Money Laundering Regulations and the sanctions regime.
- Provides advice, support and, challenge to business areas on the effective application of systems and controls as applicable to its purpose.
- Oversees and reports on Financial Crime (money laundering and sanctions) risk (Operational Risk sub-category).
- Monitor the Society's compliance with legal and regulatory obligations on the prevention of money laundering, terrorist financing and facilitation of tax evasion. The findings of this activity are to be reported to the Society's directors together with appropriate recommendations for action.
- Ensure all colleagues who have customer contact, or access to information about customers' affairs, shall receive anti-money laundering and terrorist financing training to ensure that their knowledge and understanding is at an appropriate level, and ongoing training at least annually to maintain awareness and ensure that the Society's legal obligations are met. All appropriate colleagues will also receive training on the prevention of facilitation of tax evasion, and ongoing training at least annually to maintain awareness and ensure that the Society's legal obligations are met.
- Identify and assess the money laundering and terrorist financing risks represented by the business the Society conducts so that it can mitigate that risk by applying appropriate levels of client due diligence. Assessment of tax evasion facilitation risk is clearly defined within the Society's business-wide risk assessment process.
- When a suspicion of money laundering or terrorist financing arises, the MLRO shall ensure the Society acts promptly to determine the appropriate course of action and enable business to continue where appropriate, or to withdraw from the customer relationship if necessary, and assist colleagues in any communications with the affected customer.

Return to Table of Contents