Economic Crime Prevention Policy – Anti-Money Laundering and Counter Terrorist Financing

Summary for Third Party Suppliers

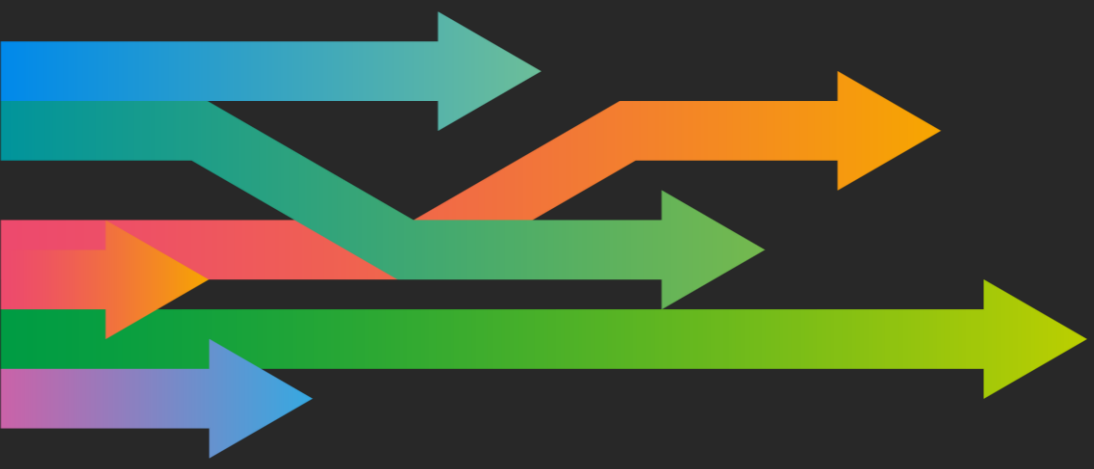

Table of Contents

Version	Effective Date
1.0 – New Template	03 November 2025

1. Rationale/Purpose

Group Policy Rationale

This Policy Summary has been designed to assist in managing the risks of Economic Crime, specifically those linked to Money Laundering, Terrorist Financing, the financing of the proliferation of weapons of mass destruction and the Facilitation of Tax Evasion which are serious threats to security and the integrity of the financial system. The overall risk includes the following risk drivers:

- Failure to comply with legal and/or regulatory responsibilities in relation to Anti Money Laundering, Counter Terrorist Financing & Counter Proliferation Financing;
- Failure to deter and detect those who would seek to use the Group to facilitate the movement of criminal funds and funds designed to finance terrorism; and/or proliferation of weapons of mass destruction;
- Failure to prevent the facilitation of Tax Evasion.

In addition, this Policy has been designed to support compliance with the following legislation and / or regulations (not exhaustive list):

- Proceeds of Crime Act 2002;
- Anti-terrorism, Crime and Security Act 2001;
- The Money Laundering, Terrorist Financing (Amendment) (EU Exit) Regulations 2020;
- Counter Terrorism Act 2008;
- The Criminal Finances Act; and
- System and Control (SYSC) Rules of the FCA Handbook.

The Economic Crime Prevention Policy is a mandatory requirement for all businesses, divisions and legal entities within the Group and applies to all colleagues (temporary and permanent) in all jurisdictions in which the Group operates. The Policy clearly articulates a set of minimum standards and requirements that meet and often exceed UK regulatory and legislative obligations and industry guidance such as that provided by the Joint Money Laundering Steering Group (JMLSG).

In jurisdictions where the local legislative and regulatory requirements exceed the requirements set out in this document, the Supplier must comply with any higher standards.

Customer Impact

The Group's vision is to be the best bank for customers. The Group's Economic Crime Prevention Policy supports this vision with the aim of providing investors with strong, stable and sustainable returns by helping to maintain the financial stability of the Group. The Policy also gives our investors and customers' confidence in the strength and integrity of the Group's compliance with legal and regulatory requirements. This is achieved by providing:

- Clarity on the Economic Crime Prevention Policy, ensuring that the Group minimises the risk of its products, services or colleagues being used to launder the proceeds of crime, fund terrorism or facilitate Tax Evasion;
- Guidance on the risk-based training programme which allows colleagues to serve its customers in line with legislation and regulation; and
- Guidance which allows businesses to implement internal processes and controls including appropriate Customer Due Diligence, effective customer screening and transaction monitoring processes.

2. Scope

An external party supplying services to the Group or performing services on the Group's behalf will be expected to comply with the Group's Economic Crime Prevention Policy where those services form part of the Group's regulated activities.

In all other circumstances, this Policy is not applicable to third-party suppliers of goods or services to the Group.

Typical circumstances that **will** result in the AML/CTF requirements of the Economic Crime Prevention Policy being applicable include the following services:

- On-boarding or introducing customers;
- Processing customer transactions;
- Providing the Group's financial products to customers; and
- Providing risk, compliance or audit services to the Group.

Typical circumstances that **will not** result in the AML/CTF requirements of the Economic Crime Prevention Policy being applicable include:

- Providing goods to the Group;
- Performing services unrelated to the Group's regulated activities (e.g. security, transport, catering, printing, etc.); and
- Conducting activities outside the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing (Amendment) (EU Exit) Regulations 2020(or equivalent).

3. MANDATORY REQUIREMENTS

- The supplier must comply with any Legal or Regulatory obligations to which they are subject in their own right, for example, by virtue of their falling within the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing (Amendment) (EU Exit) Regulations 2020 (or equivalent).

- The supplier must not engage in any conduct that results in it, or another party:
    - concealing, disguising, converting or transferring criminal property or terrorist funds;
    - entering into, or becoming concerned in an arrangement that facilitates the acquisition, retention, use or control of criminal property terrorist funds; or funds intended for the use of proliferation of weapons of mass destruction;
    - acquiring, using or possessing criminal property; terrorist funds; or funds intended for the use of proliferation of weapons of mass destruction; or
    - facilitating Tax Evasion.

- Where the Supplier is supplying a service to Lloyds Banking Group or performing a service on behalf of the Group that forms part of the Group's regulated activities and for which Lloyds Banking Group retains accountability, the Group will define for the supplier the specific requirements of the Economic Crime Prevention Policy relevant to that service. This may include some or all of the following:
    - Assessment of money laundering, terrorist financing and proliferation financing risk;
    - Customer Due Diligence / Ongoing Customer Due Diligence (including forwarding CDD material upon request);
    - Transaction Monitoring;
    - Suspicious Activity Reporting;
    - Responding to Court Orders;
    - Provision of Management Information;
    - Staff Training; and
    - Record Keeping.

In all cases, Lloyds Banking Group will perform ongoing monitoring, oversight and assurance of the supplier's activities to ensure compliance with the Economic Crime Prevention Policy.

Training

The supplier must ensure all employees / contractors complete Anti Money Laundering, Counter Terrorist Finance & Counter Proliferation Finance training no later than 8 weeks from the commencement of their employment and annually thereafter to understand how the requirements of relevant anti money laundering legislation and this Policy Summary affect their role and individual responsibilities.

Where employees are identified as working in roles considered high risk for Money Laundering, role specific training should be considered to ensure that employees are aware as to the increased Money Laundering risks associated with their roles.

4. KEY CONTROLS

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**

Anti-Money Laundering & Counter Terrorist Financing Training Third Party Suppliers must ensure that all staff (new and existing staff) complete Anti Money Laundering, Counter Terrorist Finance & Counter Proliferation Finance Training within the appropriate timescales.	1. AML/CTF/CPF training program in place. 2. Management Information (MI): • Number of staff expected to complete annual training; • Number of staff who have completed annual training; • Number of new staff expected to complete training no later than 8 weeks from the commencement of their employment • Number of new staff who have completed training no later than 8 weeks from the commencement of their employment; • Ensure evidence is available upon request by the Group supplier manager.	1. Annual review or any changes in applicable regulation/legislation. 2. Annually
Completion of New to Bank Customer Due Diligence (CDD) including Enhanced Customer Due Diligence (EDD) (where applicable) Third Parties must ensure due diligence is in place (commensurate to the level of risk) to cover all aspects of CDD and EDD (including beneficial owners) in line with the requirements of prevailing Money Laundering Regulations.	1. Sample checking of New to Bank Due Diligence records. 2. MI: • Number of accounts opened; • Number of accounts sampled; • Number of failures e.g. where the correct level of due diligence cannot be evidenced.	Monthly
Ongoing Customer Due Diligence (ODD) Third Parties must conduct ongoing monitoring of customer	1. Sample checking of ODD records. 2. MI:	Monthly

relationships to ensure existing records remain up to date.	• Number of accounts subject to ODD review; • Number of ODD cases sampled; • Number of failures e.g. where completion of ODD cannot be evidenced or is incomplete.	
Politically Exposed Persons (PEPs) Third Parties must have appropriate systems and procedures to identify where a new or existing customer relationship (including beneficial owner) is a PEP.	1. Customer screening must be in place to identify PEPs at new to bank (NTB) or where an existing relationship may become categorised as a PEP. 2. MI: • Number of PEP relationships identified.	1. Screening must be performed: • NTB within 24 hours; • Existing customers - daily screening. 2. Monthly.
Suspicious Activity Reporting (SAR) Third Parties must ensure that where knowledge or reasonable suspicion exists that a person has been engaged in money laundering, proliferation financing or has identified that criminal / terrorist property exists the Third Party must ensure that a suspicious activity report is made to the appropriate Nominated Officer.	1. Suspicious activity reports - Procedures must be in place that provide a mechanism for reporting internal suspicion when operating in the course of business. 2. MI: • Number of suspicious activity reports raised.	1. Procedures reviewed at least annually 2. Monthly.
Record Keeping Third Parties must ensure that information relating to CDD including transactional data is retained in accordance with prevailing UK Money Laundering Regulations and retrievable upon request within agreed timescales.	1. Procedures in place that ensure documentation retained (whether physical or electronic) is accurate, legible and kept for an agreed period of time. It must include the mechanism for retrieval to agreed timescales. 2. MI: • Number of instances where requests for information have not been met.	1. Procedures reviewed at least annually. 2. Monthly.

Governance An individual must be appointed within the Third Party who has primary responsibility for the Anti Money Laundering; Counter Terrorist Financing and Counter Proliferation Financing control framework	The appointed individual must ensure that: 1. Documented policies and procedures in relation to AML&CTF are maintained and meet regulatory and legislative obligations. 2. MI is produced that includes details on the levels of compliance in relation to: • Staff training; • Due Diligence completeness (CDD/EDD); • ODD; • PEP Screening activities; • SAR escalation activities; • Record keeping. MI must also identify where remedial action is required. 3. An independent oversight and monitoring programme is in place; 4. Governance arrangements are in place that ensure the escalation of MI and results of oversight and monitoring programme to the Third Parties Senior Management and LBG (as agreed) allowing for the effective management of ML/TF risks in a timely manner.	1. Annual review or any change in applicable regulation / legislation. 2. Monthly. 3. Annual review or ad hoc as required 4. Annual review or ad hoc as required

5. Non-Compliance

Any material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager.

The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.