Risk Policy Overview - Financial Crime

2025

The co-operative bank

Ethical then, now and always

Classification: PUBLIC

1 Introduction

1.1 Aims

The Co-operative Bank is committed to mitigating the financial crime risks it faces by establishing and implementing Board approved Policies. These Policies are underpinned by mandatory minimum standards, which drive internal controls for managing our financial crime risks.

It sets out the principles by which the Co-operative Bank Holdings Limited ('Holdings'), The Co-operative Bank p.l.c ('the Bank p.l.c') and The Co-operative Bank Finance p.l.c (together, the 'Bank') defines Financial Crime Risk, identifies processes, ownership, responsibilities and the risk oversight and guardianship required to support effective implementation across the Bank and its associated legal entities.

The Financial Crime Policies provide a framework to protect the Bank and our customers from the harms of financial crime.

1.2 Definitions

Financial crime includes Money Laundering; Terrorist Financing; Financial Sanctions breaches; Proliferation Financing; Fraud (internal and external); Tax Evasion or the Facilitation of Tax Evasion; Bribery; Corruption; Modern Slavery; and Human Trafficking.

- Money laundering (ML) is the process by which criminals introduce funds into the financial system, in order to disguise their origins and to create a seemingly legitimate source of money that they can then use for whatever purpose they wish.
- Terrorist financing (TF) is defined as providing financial support, in any form, to those who encourage, plan or engage in terrorism. TF can differ from ML in that the source of funds may be legitimate, such as an individual's salary or donations from the public, as well as from illegitimate sources. The aim of those financing terror is to take funds from these various sources to be channelled into terrorist organisations, without detection.
- Financial Sanctions (FS) are applied by governments or international organisations (such as the United Kingdom, United States, United Nations and the European Union) to exert pressure on regimes, entities, groups or individuals, to seek to change their behaviour. Sanctions may comprise a variety of measures including financial restrictions (such as asset freeze or prohibitions on the provision of finance), arms embargoes and trade restrictions (import and export bans). Sanctions can range from comprehensive measures aimed at a country and its ruling regime in general to targeted restrictions against named individuals, entities and vessels or can comprise of restrictions on particular activities or industry sectors.
- The Bank has zero tolerance for breaches of Sanctions rules, regulations or laws. All individuals and legal entities must comply with financial sanctions in force in their entirety.
- Proliferation Financing (PF) means the act of providing funds or financial services for use in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons in contravention of a relevant financial sanctions obligation.
- Fraud is defined as an act of deception intended for personal gain or to cause a loss to another party.
- Internal or employee fraud is defined as fraud that is committed against a company or organisation by a person who is working for it and may be perpetrated by employees, contractors or consultants. Examples of internal fraud include theft from customer accounts, payment fraud, procurement fraud, travel and subsistence fraud, personnel management fraud, receipt fraud and the exploitation or misuse of Bank assets and information.
- External fraud is defined as fraud committed against the Bank or its customers and can be perpetrated in a number of different ways. Customers can be manipulated into disclosing

credentials they should not, which allows fraudsters to access their information and finances (Account Takeover Fraud), or are coerced into performing a transaction themselves under false pretences (Authorised Push Payment Fraud). Different techniques using varying levels of sophistication across a range of different fraud types are used. Ultimately, the action results in a loss to the customer and/or Bank. In October 2024, the Payments Systems Regulator (PSR) introduced mandatory reimbursement for victims of APP fraud alongside increased transparency and data sharing. External fraud can also occur as the result of making a false representation or failing to disclose information of relevance, for example when making an application for a product. Fraud evolves continually with new types of modus operandi designed to trick and manipulate customers.

- The Failure to Prevent Fraud Offence (FtPF) as introduced by the Economic Crime and Corporate Transparency Act makes the Bank liable if it fails to prevent a specified fraud offence from being committed where: (i) an employee or agent commits the fraud; and (ii) the fraud is intended to benefit the organisation or a person to whom services are provided on behalf of the organisation.
- The offence of facilitation of tax evasion is defined within the Criminal Finances Act 2017 as being committed by an organisation where tax evasion is facilitated by a person acting in the capacity of an associated person. For the offence to apply, the associated person must deliberately and dishonestly take action to facilitate tax evasion by the taxpayer.
- Bribery is defined as the specific offence that concerns the practice of offering something, usually money, to gain an illicit advantage, including facilitation payments which are a form of bribery involving making payments or gifts to government officials in order to expedite or circumvent administrative processes.
- Corruption is defined as an abuse of a position of trust in order to gain an undue advantage.
- Modern Slavery is defined as occurring when a person holds another person in a position of slavery, servitude forced or compulsory labour.
- Human Trafficking is defined as the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of abuse of power or a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control of another person for the purpose of exploitation.

2 Application and Sources of Risk

2.1 Application

This Financial Crime Policies apply to:

- All business units and functions within the Bank
- All regulated entities, including any subsidiaries or Joint Ventures in which the Bank has a 50% or greater interest
- All employees of the Bank, including employees of any subsidiary in which the Bank has a controlling interest
- All organisations and people working on behalf of the Bank
- Third Parties as detailed below in section 2.2.1

2.1.1 Third Party Suppliers

The Bank retains ultimate responsibility for the activities of third party suppliers where financial crime requirements are outsourced or third party systems or data support these. The Bank must ensure that outsourced functions and other suppliers are fulfilling the Bank's financial crime requirements. This Policy applies to all Third Party suppliers engaged by the Bank in any activity that presents a risk of Bribery & Corruption (B&C) taking place.

Sources of Risk and Scope

2.2.1 Sources of Risk

Failing to prevent the use of products and services to facilitate financial crime exposes firms to reputational, legal and regulatory risks. Senior management has a responsibility to ensure that the Bank's systems and controls are appropriately designed and implemented and that they operate effectively to manage risks in line with legal expectations, as well as considering any reputational risks arising through association with individuals or entities connected with financial crime.

2.2.2 Risks in Scope

The scope of the Bank's Financial Crime Policies extends to all financial crime risk exposures. The Bank must implement and operate appropriate systems, procedures and controls to comply with the Bank's legal and regulatory financial crime requirements and guidance, most notably outlined in, but not limited to:

- The Proceeds of Crime Act 2002 (as amended) by the Crime and Courts Act 2013 and the Serious Crime Act 2015), which applies to the proceeds of all crimes including tax evasion
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on Payer) Regulations (MLR) 2017 as amended by the MLR 2022
- The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001, the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)
- The Bank complies with the requirements of those sanctions regimes to which it is subject (these include UK, UN, EU & OFAC)
- Financial Services and Markets Act 2000(FSMA)
- The Bribery Act 2010
- The Criminal Finances Act 2017
- The Immigration Act 2016
- The Failure to Prevent Fraud Offence (FtPF) as introduced by the Economic Crime and Corporate Transparency Act 2023

The Bank also follows guidance and industry standards as set out in, but not limited to:

- The Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector on the prevention of money laundering/combating terrorist financing
- HMT Treasury advisory notices
- The Financial Action Task Force (FATF) Recommendations
- UK National risk assessment of money laundering and terrorist financing
- FCA Sourcebook of rules and guidance, in particular, the Senior Management Arrangements, Systems and Controls (SYSC)
- Financial Crime – A Guide for Firms
- BSI PAS 17271 Code of Practice

To accompany the Financial Crime Policies, the Bank has control standards, created and maintained by 2LOD, and procedural guidance documents, maintained by 1LOD with 2LOD oversight.

To ensure that financial crime risks are managed effectively; this Policy requires the Bank to do the following:

- Appoint a Money Laundering Reporting Officer (MLRO). The MLRO reports directly to the Chief Risk Officer (CRO) and provides regular updates to the Board Risk Committee. The MLRO holds overall responsibility for the creation and maintenance of effective AML systems and controls.
- Identify, assess, and understand the financial crime risks to which the Bank is exposed and take the appropriate mitigation measures in accordance with the level of risk.
- Conduct annual risk assessments of the ML, TF, FS, & PF, Internal Fraud & Anti-Bribery and Corruption

(including facilitation of tax evasion) and External Fraud risks that are relevant to the Bank and its business model. A copy of the AML Regulatory Risk Assessment must be available to the Financial Conduct Authority (FCA) upon request

- On-board all customers through a risk-based identification, verification and due diligence process. This is the first stage in the process of knowing and understanding the customer and assists with setting expectations of future activity, which helps in the assessment of the money laundering risk that they may pose. The Bank will use electronic verification systems to identify and verify customers where possible.
- Embed controls to mitigate the risks of providing funds, economic resources or financial services to individuals and entities subject to UK, EU, US or UN sanctions.
- Provide on-boarding training for all new joiners and, on an annual basis as a minimum, refresher training to all employees including senior management. Colleagues whose role carries an elevated risk must receive more specific training and assessment. Training material is reviewed on an annual basis.
- Identify appropriate management information (MI), metrics and tolerances to facilitate the oversight and reporting of the Bank's performance in relation to the detection, prevention, identification and reporting of financial crime risks.
- At least annually the MLRO will provide the Board with a report on AML, CTF, FS and B&C performance across the Bank.
- Provide timely and accurate data to meet regulatory reporting requirements.
- Ensure that new customers who undertake activities prohibited by the Bank's Board are not allowed to enter into a relationship with the Bank and take action to terminate any existing relationships that fall into a prohibited category.
- Commit to investing in systems and people to establish proportionate Financial Crime Risk management mechanisms that balance good customer outcomes, Risk and Reward and deliver best-practice Risk Management.
- Introduce and maintain efficient and cost-effective controls and procedures to prevent, detect, deter, monitor and measure fraud.
- Implement appropriate governance to provide sufficient oversight, identification and discussion of fraud risks and issues.
- Regularly educate our customers on the fraud risks they face.
- Ensure that all colleagues act with integrity at all times and do not engage in criminal activity of any kind, even that which may benefit the company.
- Ensure that all colleagues have a clear obligation to report any actual or suspected financial crimes that they encounter during their employment, whether internal or external.
- Ensure that decision making processes reflect our values, ethics and customer first approach to ensure fairness, consistency and positive customer outcomes.
- Consider whether a customer is vulnerable when making decisions.
- Have open, honest and effective internal channels in place to ensure that staff can raise concerns about incidents, emerging issues and risks in a timely manner.
- Maintain confidentiality of information and only release information when appropriate to do so and in line with relevant controls and legislation.
- Maintain confidentiality in respect of systems and controls to prevent financial crime.
- Acts in an open and co-operative way with all regulatory and law enforcement agencies.
- Report all cases of confirmed internal fraud to the police.
- Undertake appropriate screening of new employees prior to them starting their employment and conduct ongoing screening for those colleagues specified within the Senior Manager Certification Regime (SMCR) and other higher risk positions.
- Ensure reasonable fraud prevention procedures are in place to mitigate the risk of a specified fraud offence being committed by an employee or associated person, for the Bank's benefit.

3 Roles and Responsibilities

The Bank's Three Lines of Defence (3LOD) governance model is designed to ensure appropriate responsibility and accountability is allocated to the management, reporting and escalation of risk.

3.1 First Line of Defence (1LOD)

All Executives and Senior Leaders are responsible for the management of Risk. As part of the Senior Manager & Certification Regime (SM&CR) specific accountabilities are defined. Below are specific requirements, over and above the responsibilities set out in the RMF Policy, of the 1st LOD in relation to this Risk type.

The management and control of financial crime risk is owned by the first line of defence.
The high-level financial crime related responsibilities of all Executive members and their leadership teams include but are not limited to the following:

- Providing the tone from the top and promoting a zero tolerance approach to financial crime across the Bank, managing within risk appetite and allocating resources appropriately
- Understanding their accountabilities and promoting a compliant culture across the business area
- Developing and implementing appropriate control and mitigation strategies to manage identified financial crime risks within agreed Risk Appetite and
- Liaison with the regulator / other external bodies as appropriate

3.2 Second Line (The Risk Function)

The Bank's Compliance and Risk Functions act as the second line of defence (2nd LOD). 2nd LOD are accountable for ensuring there is an appropriate RMF and for oversight and guardianship, challenging and monitoring the implementation of the RMF. 2nd LOD are also responsible for designing methods and tools employed for Risk Management purposes and overseeing the implementation of these.

3.3 Risk Framework Owner (RFO)

The RFO (MLRO) is accountable for ensuring there is an appropriate risk framework and for providing oversight and guardianship by challenging and monitoring the implementation of the risk framework and underlying Policies and Control Standards. The RFO develops the framework for financial crime risk in line with the RMF, defines appetite (with 1st LOD input) for Board approval and is responsible for the Financial Crime Risk Policies, measurement, oversight and assurance.

Key responsibilities include the following:

- Promoting a strong financial crime risk culture across the Bank
- Creating and maintaining Financial Crime Policies and Control Standards
- Communicating, educating and advising across the Bank on financial crime Risk
- Ensuring Risk Appetite and core measures are set, agreeing appetite and communicating and monitoring Risk Appetite
- Collaborating with Executives and their Leadership Teams to implement and improve financial crime risk management processes and controls and to agree controls and processes
- Liaison with the regulator and other external bodies as appropriate

3.4 Third Line of Defence

Internal and External Audit act as the third line of defence (3rd LOD). They independently monitor the embedding of the RMF and report on progress to the Executive and Audit Committee. On an ongoing basis, Internal Audit will form an independent view on the Bank's management of risk, based on BAU audit work, issue assurance and business monitoring. This will include activity of both the 1st LOD and the 2nd LOD.

4 Compliance

All areas of the Bank are expected to evidence compliance with Financial Crime Policies and Control

Standards unless specifically excluded within the Scope section.

4.1 Waivers and Dispensations

No waivers (permanent exceptions) will be agreed outside any area excluded within the Scope section of the Financial Crime Policies.

A temporary dispensation is the action / decision to exclude temporarily a Business Unit, process or activity from the scope / requirements / principles of all or parts of the Policy. This will increase the risk profile and the likelihood is this will result in a specific risk outside appetite. Requests must be sent to the appropriate RFO setting out the rationale, expected impact and duration.

An Issue must be raised in the Bank's Operational Risk Management System with an action plan designed to achieve compliance. Where there is no action plan and therefore the risk falls into the criteria of a risk acceptance, the Bank's Risk Acceptance process must be followed.

4.2 Breaches

A breach is classified as non-compliance with any requirement of Policy where there is no approved modification or exception in place. In situations where breaches of Policy arise, it is essential that there are clearly defined, efficient and appropriate processes to get the risk back within appetite and this should be made clear in an Issue and Action plan. The RFO must be informed of any breaches who will escalate a confirmed breach through governance.

5 Policy Ownership and Approval

Financial Crime Policies are owned by the MLRO/Head of Financial Crime and approved by the Operational, Compliance and Financial Crime Risk Oversight Committee (OCROC).