Fraud Risk Policy Overview

2022

The co-operative bank

Contents

1 Introduction 3

1.1 Aims 3

1.2 Definition 3

2 Risk Appetite, Application and Sources of Risk 3

2.1 Application 3

2.1.1 Third Party Suppliers 3

2.2 Sources of Risk and Scope 4

2.2.1 Sources of Risk 4

2.2.2 Risks in Scope 4

3 Policy Requirements 4

3.1 Risk Identification and Measurement 5

3.2 Risk Management 5

3.3 Risk Monitoring and Reporting 6

4 Compliance 6

4.1 Waivers and Dispensations 6

4.2 Breaches 6

1 Introduction

1.1 Aims

The purpose of this Policy is to establish a principle for managing Fraud Risk throughout the Bank. 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 Fraud Risk, identifies processes, ownership, responsibilities and the risk oversight and guardianship required to support effective implementation across the Bank and its associated legal entities.

1.2 Definition

The agreed definition of Fraud Risk is as follows:

The risk that the Bank is exposed to uncontrolled levels of financial crime resulting in unplanned fraud losses, reduced customer confidence and reputational damage.

2 Risk Appetite, Application and Sources of Risk

2.1 Application

This Policy applies 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

Business areas own the relationship with third party suppliers and their responsibilities in respect of the Fraud Policy are to ensure suppliers:

- Institute and maintain cost effective policies and procedures based on risk to deter fraud against the Bank and its customers.

The Bank retains ultimate responsibility for the activities undertaken by outsource providers, to ensure that they fulfil fraud requirements. Policies are required to be assessed in line with this policy prior to any relationship being established and also included in ongoing reviews of such relationships.

2.2 Sources of Risk and Scope

2.2.1 Sources of Risk

The key sources of Fraud Risk include but are not limited to

- Internal Fraud e.g.
    - o Theft of customer or Bank assets by an employee(s)
    - o Theft of customer data
    - o Overstating expense claims

- External Fraud e.g.
    - o Card Fraud
    - o Account Takeover Fraud
    - o Cheque Fraud
    - o Mortgage Fraud
    - o Investment Fraud
    - o Facilitation of Tax evasion
    - o Authorised Push Payment (APP) scams

- Bribery and corruption e.g.
    - o Bribing another person
    - o Being bribed
    - o Bribing a foreign public official
    - o Failure of the Bank to prevent bribery

2.2.2 Risks in Scope

This Policy reflects, all legal and regulatory requirements and guidance, most notably outlined in but not limited to:

- FCA Sourcebook of rules and guidance
- 'Financial Crime – A Guide for Firms'
- Financial Services and Markets Act 2000(FSMA)
- The Bribery Act 2010
- The Criminal Finances Act 2017
- The Immigration Act 2016
- BSI PAS 17271 Code of Practice
- CRM Code – Lending Standards Board

3 Policy Requirements

The Bank is committed to investing in systems and people to establish proportionate fraud risk management mechanisms that balance good customer outcomes, risk and reward and deliver best-practice risk management.

It is our policy that:

- Efficient and cost effective controls and procedures are introduced and maintained to prevent, detect, deter, monitor and measure fraud
- The Bank will educate our customers on the fraud risks they face

- All colleagues act with integrity at all times and do not engage in fraudulent activity of any kind, even that which may benefit the company
- All colleagues receive training appropriate to their role
- All colleagues have a clear obligation to report actual or suspected fraud both internal and external
- Decision making processes reflect our values, ethics and customer first approach to ensure fairness, consistency and positive customer outcomes. Consideration is given to whether a customer could be considered vulnerable
- Open, honest and effective internal channels (e.g. the 'whistle blowing' process) are in place to ensure staff raise concerns about any incidents, emerging issues and risks are raised in a timely manner
- Confidentiality of information is observed and information must only be released when appropriate to do so and in a controlled environment
- Confidentiality in respect of systems and controls to prevent fraud must be maintained
- The Bank acts in an open and co-operative way with all appropriate regulatory and law enforcement agencies
- All cases of confirmed internal fraud will be reported to the police
- Only specialist individuals release information to the police and law enforcement agencies
- The Bank undertakes appropriate screening of new employees prior to them starting their employment and ongoing screening for those colleagues specified within the Senior Manager Certification Regime (SMCR) and other higher risk positions.

3.1 Risk Identification and Measurement

Any significant risks must be managed, monitored and reported as part of business as usual management, and through Bank governance.

New or changed underlying risks must be identified through assessment of internal and external environmental changes, regulatory changes, horizon scanning, risk events and the Risk & Control Self-Assessment (RCSA) process.

3.2 Risk Management

Levels of authority must exist to support the management of fraud risk at the Bank and business unit level

- Processes must exist for choosing to accept, avoid, transfer or mitigate fraud risk in accordance with the stated risk appetite and the defined levels of authority, by following the Bank's Risk Acceptance Process
- A process must exist for identifying and managing changes to the fraud risk profile of the Bank
- A process must exist for identifying and managing emerging risks that affect the fraud risk profile of the Bank including any fraud risks associated with Climate change
- A process must exist for ensuring the Bank meets industry and regulatory best practice guidelines
- Processes and controls, with defined ownership, must exist to mitigate fraud risk to levels that are consistent with the stated risk appetite

3.3 Risk Monitoring and Reporting

- Exposure to fraud risk must be monitored on a regular basis
- Fraud rule performance must be regularly reviewed including any significant changes in experience relative to assumptions made, and the impact of this
- Monitoring including a forward looking assessment and leading indicators
- Relevant external information or intelligence must be identified and should, where appropriate, be monitored to inform decision making and assumptions
- Corrective action plans must be implemented where there are actual or potential breaches of risk appetite
- Assurance activity, using a risk-based approach, to establish the operational effectiveness of controls to mitigate fraud risk must be undertaken
- Evidence of how the Bank is managing its fraud risks in relation to its risk appetite must be provided
- Information must be provided to meet internal and external reporting requirements in line with relevant Policy and/or legal and regulatory requirements
- Regular reporting of key metrics/other measures for monitoring control effectiveness and risk exposures against appetite must be undertaken
- Provision of aggregated fraud risk reporting for the Bank
- Regular reporting of progress against corrective actions plans that are mitigating risk outside of fraud risk appetite must be undertaken
- All defined fraud risk reporting must be provided in a timely, accurate and complete manner
- All material exceptions must be reported promptly to the appropriate person and/or forum
- Threats to achievement of business objectives and targets from existing issues and emerging risk exposure must be reported in a timely, accurate and complete manner
- Evidence of compliance with the Control Standards, and senior business management assurances, must be provided through the Risk and Control Self-Assessment process and the Control Standard Gap Analysis Process
- Any instances of significant Policy breaches and control weaknesses must be escalated to the appropriate governance committee

4 Compliance

All areas of the Bank are expected to evidence compliance with this Policy 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 this Policy. A temporary dispensation for the purpose of this Policy 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.

4.2 Breaches

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