# Risk Policy Overview - Conduct Risk

2023

The co-operative bank

# 1 Introduction

## 1.1 Aims

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

This Policy forms part of the Risk Management Framework (RMF). The RMF consists of Risk Policies, Risk Appetites, Control Standards and Business Unit Operating Procedures. Bank's risk taxonomy forms part of the RMF and each Risk defined within the RMF has a Policy and one or more Control Standards to support it. Some Control Standards are supported by Bank wide procedures.

## 1.2 Definitions

The agreed definition of Conduct Risk is as follows:

Conduct Risk is defined as the risk that the Bank's behaviours, products or services will result in poor outcomes or harm for customers.

# 2 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 and sub-contractors as detailed below in section 2.2.1

### 2.1.1 Third Party Suppliers

The whole of this Policy applies to third parties and sub-contractors engaged in any activity on behalf of the Bank that impacts our customers. They need to comply with the Financial Conduct Authority (FCA) or any voluntary codes / guidelines the Bank has signed up to, during the provision of those activities or services. However the Bank must have systems and controls in place to monitor the arrangements with the third party and provide assurance that it is meeting its regulatory obligations and delivering good outcomes.

## 2.2 Sources of Risk and Scope

### 2.2.1 Sources of Risk

While it is good business to deliver good customer outcomes, service and market conduct, it is the FCA which sets the scope in terms of what is ultimately expected in relation to Conduct Risk. Material failures would be subject to investigation and potential fines. Risks and processes which have not been effectively identified, assessed and mitigated can result in Conduct Risk. The sources of these risks can vary from internal and external forces and include:



Classification: PUBLIC

- Poor products (design and processes)
- Poor customer communication
- Poor customer interaction
- Human error
- Poor system design
- Staff behaviour
- Lack of staff training
- Inadequate monitoring
- Lack of governance / controls
- Changes in regulatory expectations
- Activities of 3rd or 4th parties acting on the Bank's behalf

### 2.2.2 Risks in Scope

For the purpose of this Policy, the relevant risks are principally those associated with any failure that results in poor customer outcomes or customer harm, which may lead financial loss and / or reputational damage. In addition to the operational aspects of the product lifecycle, the Bank's business model and strategy must put the customer at the heart of the business and allow for reasonable adjustments where appropriate. This can be further explained by the four consumer outcomes in the Consumer Duty below.

| Consumer Duty Outcome | Activity |
|---|---|
| Products and Services | ▪ Ensure that the design of the product or service meets the needs, characteristics and objectives of customers in the identified target market<br>▪ Ensure that the intended distribution strategy for the product or service is appropriate for the target market<br>▪ Take account of any particular additional or different needs, characteristics and objectives that might be relevant for customers in the target market with characteristics of vulnerability<br>▪ Carry out regular reviews to ensure that the product or service continues to meet the needs, characteristics and objectives of the target market |
| Price and Value | ▪ Ensure there is a reasonable relationship between the price a customer pays for a product or service and the benefits they receive from it<br>▪ Ensure that its products provide fair value to customers in the target markets for those products<br>▪ Carry out a value assessment of its products and review that assessment on a regular basis appropriate to the nature and duration of the product |
| Consumer Understanding | ▪ Support our customers' understanding by ensuring that their communications meet the information needs of customers, are likely to be understood by customers intended to receive the communication, and equip them to make decisions that are effective, timely and properly informed<br>▪ Tailor communications taking into account the characteristics of the customers intended to receive the communication – including any characteristics of vulnerability, the complexity of products, the communication channel used, and the role of the firm<br>▪ When interacting directly with a customer on a one-to-one basis, where appropriate, tailor communications to meet the information needs of the customer, and ask them if they understand the information and have any further questions<br>▪ Test, monitor and adapt communications to support understanding and good outcomes for customers |



Classification: PUBLIC

| | |
|---|---|
| Consumer Support | ▪ Design and deliver support that meets the needs of customers, including those with characteristics of vulnerability<br>▪ Ensure that customers can use their products as reasonably anticipated<br>▪ Ensure they include appropriate friction in customer journeys to mitigate the risk of harm and give customers sufficient opportunity to understand and assess their options, including any risks<br>▪ Ensure that customers do not face unreasonable barriers (including unreasonable additional costs) during the lifecycle of a product or service<br>▪ Monitor the quality of the support they are offering, looking for evidence that may indicate areas where they fall short of the outcome, and act promptly to address these, and<br>▪ Ensure they do not disadvantage particular groups of customers, including those with characteristics of vulnerability |

## Colleague Behaviour

"Conduct" also goes beyond pure customer outcome assessment and individuals need to observe appropriate behaviours, which include work related and external activities. FCA "Conduct Rules" (COCON) rulebook formalises the need and responsibility for colleagues to act:

- with integrity, and due skill, care and diligence
- in an open and co-operative manner with the PRA and FCA
- with due regard to the interests of customers and treat them fairly
- observe the proper standards of market conduct

# 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 1st Line of Defence (LOD)

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. The appendix within the RMF Policy lists these key accountabilities. 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 First Line of Defence (1st LOD) Business Areas are responsible for the day to day management of Conduct Risk, including but not limited to:

- Identifying, assessing and reviewing on an ongoing basis all Conduct Risks (including emerging risks)
- Measuring and managing the risks identified through the collection of MI and data. Reviews need to be initiated where MI / data highlights issues and/or improvements
- Ensuring that adequate controls and metrics are implemented and embedded to identify, manage, monitor and report on risks
- Monitoring includes conducting Post Implementation Reviews (PIRs), Annual Product Reviews (APRs) and using the outcomes to inform product development and change processes
- Reporting any breach of this Policy to the RFO
- Owning the decisions implementation plans and tracking of action to manage all identified Conduct Risks or issues to remain within risk appetite

## 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 is also responsible for designing methods and tools employed for Risk Management purposes and overseeing the



Classification: PUBLIC

implementation of these.

## 3.3 Risk Framework Owner (RFO)

Compliance support the Risk Framework Owner to develop the Framework for Conduct Risk in line with the RMF, including:

- Upkeep of the Risk Policy and necessary Control Standards
- Defining risk appetite and measurement
- Implementing appropriate oversight and assurance

Compliance provide oversight and challenge to the 1st LOD management of Conduct Risk on a risk based resource allocation to:

- Provide forward looking assessment and challenge where appropriate to ensure Conduct Risk appetite is considered and incorporated in Strategic and Business planning
- Review and evaluate all aspects of risk identification
- Provide expert advice on Regulatory and Conduct Risk issues
- Undertake reviews to ensure Conduct Risks are managed effectively and in accordance with this Policy
- Provide review and challenge over all Products to ensure that relevant risks have been identified and assessed and appropriate risk mitigation techniques defined, including any third party product and any outsourcing arrangement
- Support New Product and Product Change Risk Assessments and Product Reviews by providing advice, guidance and technical input as required • Review and challenge the results of Product Post Implementation Reviews (PIRs) and Annual Product Reviews (APRs)
- Review and where appropriate, challenge the effectiveness of the 1st LOD's monitoring, reporting and resolution of breaches of risk appetite or Policy

## 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 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. 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 Archer 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 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 and this should be made clear in an Issue and Action plan



Classification: PUBLIC

raised in Archer as part of the RCSA process. The RFO must be informed of any breaches who will escalate a confirmed breach through governance.

# 5 Policy Ownership and Approval

This Policy is owned by the Director of Compliance and approved by Operational, Compliance and Financial Crime Risk Oversight Committee.



Classification: PUBLIC