Information and Data Risk Policy Overview

2024

Data classification: Public

The co-operative bank

Ethical then, now and always

1 Introduction

1.1 Aims

The purpose of this Policy is to establish a principle for managing Information and Data Risk throughout the Bank. It sets out the principles by which the Co-operative Bank defines Information and Data Risk. The Policy forms part of the Risk Management Framework (RMF). The RMF consists of Risk Policies, Risk Appetites, Control Standards and Business Unit Operating Procedures.

At the heart of the Bank's approach to Information and Data risk is the protection of our customer's data. It aims to avoid causing material detriment to the Bank whilst ensuring data is of sufficient quality to enable accurate and timely data-driven business decisions and a positive customer experience.

1.2 Definitions

The Bank defines Information and Data Risk as follows:

- The risk of direct or indirect losses arising from the theft, loss or misuse of data, or the processing of poor quality Information and Data facilitated by inadequate data management, information security and/or data protection resulting in customer or financial detriment, legal or regulatory censure, and/or ill-informed business decisions.

Note; the words Information and Data are often used interchangeably however there are clear distinctions and it is therefore important to understand these differences. That said, the approach to risk management of both is closely related and will be reflected as such in the Policy.

Data is defined as facts or figures which are efficient for movement or storage — bits of information, but not information itself. Whereas information is defined as data that has been organised for a specific purpose in context to a particular event or subject (such as a customer) - without data, information cannot be processed.

Data 'Quality' relates to the Completeness, Accuracy and Validity of the data. "Information Risk" and "Data Risk" are closely related but not always directly synonymous. The policy covers Information and Data held in all forms, e.g. electronic, paper.

2 Application and Sources of Risk

2.1 Application

The 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 whether permanent, contract or temporary, including employees of any subsidiary in which the Bank has a controlling interest
- All organisations and people working on behalf of the Bank

2.1.1 Third Party Suppliers

This Policy applies to all Third Party suppliers engaged by the Bank who produce, access, transform, transfer, store, consume or delete the Bank's Data and Information.

2.2 Sources of Risk and Scope

2.2.1 Sources of Risk

Example sources of risk include, but are not exclusive to:

- The creation of inaccurate data at the point of input to customer facing systems by users or other systems.
- Public release of data or information either accidentally or with malicious intent.
- Sharing or use of personal details (customer or colleague) outside of regulation and compliance.
- Potential unauthorised access and/or loss of data.
- Failure or corruption of a data storage device which holds vital operational data.
- Failure of data feeds or integration processes connecting data infrastructure and external feeds.
- Failure to identify the information and data impacts associated with change initiatives.
- Loss of data or inaccurate processing of data to due inadequate End User Computing (EUCs) controls

These sources of risk can crystallise with the following example impacts;

Customer Impact - arising from poor data quality preventing appropriate regulatory communication or leading to customer data being compromised

Operational Impacts - arising from lack of data availability, failure of integration process and poor security controls leading to failure of operational/customer facing systems and possible security breaches.

Financial Impacts - arising from an ineffective control environment (including data protection and security controls) resulting in data breaches, increased regulatory oversight and ultimately financial penalties.

Regulatory Impacts – arising for incorrect data in Bank submissions and Regulatory censure as a result of failures in managing personal data.

Reputational Damage - arising from poor data quality and limited systems integration resulting in a poor experience for customers at on-boarding and through their customer lifecycle.

2.2.2 Risks in Scope

The scope of the Policy covers all aspects of Information and Data related activity across the Bank, irrespective of business function. This includes but is not exclusive to:

- **Data Governance** - risks associated with an ineffective data control framework including governance structure, ownership, policies, procedures, processes and controls.
- **Data Development** – risks associated with the data development lifecycle focused on defining data requirements, designing the data solution components, and implementing these

components. This also includes risks associated with misaligned data architecture, strategic alignment and data strategy.

- **Data Management** - risks associated with data loss, data availability, data storage, data quality and data usage
- **Information Security and Privacy** - risks associated with the preventative measures to prevent unauthorised access to information and data.
- **Data Protection & Compliance** - risks associated with safeguarding personal information and data against breaches, corruption or loss either in transit or at rest. Including risks associated with non-compliance of internal and external mandatory regulation, legislation and standards.

We also comply with the laws and regulations on the destruction of personal data, ensuring it is retained only for as long as necessary and is destroyed appropriately and safely, is classified appropriately and the creation and processing of data ensures the accuracy and integrity of that data throughout its lifecycle from creation to destruction. The Bank aims to keep data no longer than is required in line with UK Data Retention requirements.

Regulations in scope (including but not limited to);

- UK General Data Protection Regulation
- Data Protection Act 2018
- Privacy and Electronic Communications Regulation
- ISO27001 Information Security Standard

2.3 Specific mitigation to ongoing risk

2.3.1 Data Privacy and Security

- Commitment to notify data subjects in a timely manner in case of policy changes or data breach
- Commitment to require third parties with whom the bank data is shared to comply with the company's Information and Data policy

2.3.2 Data Request Management

- Commitment to respect human rights in data management
- All governmental data requests to be managed by strict senior management oversight
- Notification of data subjects in case of any changes to data sharing under legal requirements
- Commitment to Incident investigation and corrective action where concern is raised around data requests
- Commitment to ensure that there are remedies for victims of human rights violations if they occur as a result of the company's data sharing practices
- All data requests by law enforcement or government are evaluated in line with both lawful and ethical guidelines

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 risks.

3.1 1st 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 1LOD in relation to this Risk type.

- The production and maintenance of a Bank Data Strategy
- Executive Sponsors, Business Sponsors and Business Leads are accountable for the data they own in line with the Data Strategy
- The Bank's Data Governance function is responsible for ensuring that data governance, data management and data quality management frameworks are in place and monitoring adherence.
- The Bank's IT Security function is responsible for the authorship of the Banks security standards which must be adhered to by all areas of the Bank.

3.2 Second Line (The Risk Function)

The Bank's Compliance and Risk Functions act as the second line of defence (2nd LOD). 2LOD are accountable for ensuring there is appropriate oversight and guardianship, challenging and monitoring the implementation of the RMF. 2LOD is also responsible for designing methods and tools employed for Risk Management purposes and overseeing the implementation of these in liaison with the 1LOD.

The Banks Data Protection Officer (DPO) also sits in 2LOD. The DPO is responsible for advising all individuals engaged in activities with an Information and Data impact of their data protection responsibilities.

3.3 Risk Framework Owner (RFO)

The RFO in the 2nd LOD is the Enterprise and Operational Risk Director. The RFO for Information & Data Risk is responsible for:

- Defining the Policy and appropriate Risk Appetite Metrics in consultation with key stakeholders
- Providing oversight of the risk management process and challenge to first line activities including the effectiveness of risk indicators, assumptions and metrics used as well as the conclusions reached by the 1LOD in respect of levels and nature of risk taking
- Escalating any identified issues to the appropriate committee(s) in the event that issues have not been resolved during the review and challenge process
- Being part of key committee discussions to ensure regular communication and feedback is maintained with key stakeholders
- Undertaking deep dive assurance reviews to provide a detailed assessment of a particular aspect of a principal risk

3.4 Third Line of Defence

Internal and External Audit act as the third line of defence (3LOD). They independently monitor the embedding 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 1LOD and the 2LOD. Internal Audit may review specific elements of Information and Data in line with the Audit planning process, and also include within relevant wider audits.

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 is the action / decision to exclude temporarily a Business Unit, processor 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

This Policy is owned by the Enterprise and Operational Risk Director and approved by the Operational, Compliance and Financial Crime Risk Oversight Committee (OCROC).