CO-OPERATIVE BANKS DEVELOPMENT AGENCY

27th Floor, 240 Vermeulen Street • Private Bag X115, Pretoria, 0001 • Tel: 012 315 5367 • Fax: 012 315 5905 • email: CBDA@treasury.gov.za

Guidance note on Operational Risk Management

For

Co-operative Financial Institutions

Background

Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

Failure to implement proper processes and procedures to control operational risks can result in a misstatement of the co-operative financial institution's (CFI) risk/return profile and expose the CFI to significant losses.

CFIs should develop and implement a written operational risk policy (or plan for managing operational risk) tailored to their size and complexity.

This Guideline establishes the minimum standards of the CBDA Supervisors with respect to management by CFIs of operational risk. Reference should be made to the CFI Rules and Regulations, as available on the CBDA website and as amended from time to time.

Each CFI is required to implement a policy that addresses the following:

1. Defined and prudent levels of decision-making authority

1.1 Authority for corporate decisions in all areas of operations defined.

1.2 Appropriate delegation of authority defined and documented.

1.3 The skills and experience of staff are commensurate with the defined levels of authority.

1.4 Establishment of lines of reporting and areas of responsibility.

2. The security and operation of a management information system

2.1 Establishment of internal controls that protect the accuracy and security of the management information system and processes.

2.2 Transactions recorded on an accurate, complete and timely basis.

2.3 Accounting for all on balance sheet and off balance sheet activities.

2.4 Protection of the integrity of the system hardware, software and data through appropriate access and process controls.

2.5 Provision of an audit trail for all transactions.

2.6 Back up and off-site storage of data.

3. Technology development and maintenance

3.1 Establishment of an appropriate framework for technology development and maintenance, and processes for:

3.1.1 Planning for future technology requirements consistent with business strategies and business plans.

3.1.2 Identifying and evaluating technology solutions for business activities.

3.1.3 Development and/or acquisition of software.

3.1.4 Documentation, testing and implementation of software.

3.1.5 Delivery and support, including identification and solution of problems.

4. Safeguarding premises, assets and records of financial and other key information.

4.1 Establishing internal controls that will ensure:

4.1.1 Premises of the CFI are safeguarded, including protection of members and staff from exposure to crime or injury.

4.1.2 Safety and protection of assets of the CFI and assets of other parties held in its care, control and custody.

4.1.3 Safety of financial records and other key information.

5. Disaster recovery and business continuity plans

5.1 Establishment of appropriate disaster recovery and business continuity plans, including:

5.1.1 Processes to deal with short term and longer term business disruptions.

5.1.2 Nature, frequency and extent of testing backup, recovery and contingency plans.

6. Outsourcing services

6.1 Identification of:

6.1.1 The process for selecting service providers.

6.1.2 Standards for outsourced services, including accuracy, security, privacy and confidentiality.

6.1.3 The process for monitoring the performance and risks relating to outsourced services and service providers i.e. contact management.

6.2 Periodic review of outstanding contracts.

7. Monitoring controls

7.1 Establishment of appropriate controls to monitor adherence to operational risk policy, including:

7.1.1 Routines for transaction verification and validation for error detection and fraud prevention.

7.1.2 Ensuring a functional independent supervisory/audit function.

7.2 All CFIs are required to have regular reviews by the Supervisory/Audit committee, with such reports being tabled to the main board and the Supervisor.

7.3 Receiving and reviewing reports from external auditors and supervisory committee.

8. Human Resources

8.1 Appropriate segregation of responsibilities to ensure appropriate authorization levels.