FINANCIAL SERVICES COMMISSION

GUIDELINE No. 7

OPERATIONAL RISK MANAGEMENT

This Guideline is issued by the Financial Services Commission ("the Commission") pursuant to section 53 of the Financial Services Commission Act 2010-21 ("Act") and comes into effect March 1, 2013.

This Guideline establishes the standards of the Commission with respect to management by credit unions of operational risk.

Each credit union 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 credit union are safeguarded, including protection of members and staff from exposure to crime or injury.

4.1.2 Safety and protection of assets of the credit union 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 capable and reliable service providers to ensure transparency.

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.

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 Establishment of an independent internal audit function

7.2 All credit unions with assets over $10 million are required to have an internal audit conducted at least once per year.

7.3 Other credit unions with assets under $10 million may be required to have an internal audit conducted as determined by the Commission.

7.4 Receiving reports from external and internal auditors

8. Human Resources

8.1 Appropriate segregation of responsibilities