Table of Contents

Policy Objectives 1
Responsibility 1
Policy Guidelines 2
Information Technology 3
Outsourcing of Services 4
Reporting 5
Compliance 6
Policy Approval and Review 6

The policies in this chapter are sufficient for most situations that may arise. The policies may not cover each and every situation and must be customized to meet each credit union's unique requirements.

The shaded text that appears in this chapter is customizable by your credit union. When customizing this chapter, use your software's Find/Replace function to insert your credit union's name wherever "the credit union" (or a variation of this phrase) appears.

Text in boxes, such as this one, is background information, and can be deleted when you customize this file.

Note: Material from By-Law No. 5 has been incorporated into this policy. Customizing it will provide your credit union with Central's policy recommendations. It is strongly suggested that credit union managers and boards consult the workbooks prepared by DICO for additional guidance that will help them comply with the By-Law.

The credit union believes that it is in keeping with the overall credit union philosophy to have appropriate and prudent policies, procedures and controls to manage the operational risk of the institution.

Policy Objectives

To establish an overall framework of operational risk management which ensures that the credit union faces limited exposure to all material risks.

To implement a policy that addresses:

- defined and prudent levels of decision-making authority
- the security and operation of a management information system
- technology development and maintenance
- safeguarding of the institution's premises, assets and records of financial and other key information
- disaster recovery and business continuity plans
- outsourcing of services
- monitoring controls

Responsibility

The Manager/Treasurer-Manager/Chief Financial Officer is responsible for implementing operational risk management controls in accordance with this policy.

The credit union may engage outside consulting help to establish and/or maintain the ongoing requirements of this policy.

The board of directors is responsible for ensuring that any major variances to required policies and procedures are identified and that appropriate corrective actions are implemented.

Policy Guidelines

The Management/Treasurer-Manager shall develop and implement sound and prudent organizational and procedural controls in compliance with this policy and its overall operational risk management philosophy.

The credit union will maintain an organization chart which includes board committees and details lines of reporting, responsibility and authority.

A framework for approval authorities will be implemented to ensure that responsibilities and approvals for transactions are assigned to the proper and appropriate individuals and/or within the credit union.

Specific approval authorities will include:

- To whom the approval is delegated (by position or by individual)
- The absolute or incremental authority being delegated
- Restrictions, if any, placed on the authority
- Whether the person can further delegate the authority.

Appropriate segregation of responsibilities and duties will be assigned so that no one person can initiate, authorize, execute and record a transaction. Where such segregation is not possible, review and verification of such transactions shall be done on a regular basis by the Audit Committee or other individuals authorized to do so by the board of directors.

The credit union will maintain an effective information system that reports relevant information on a timely basis to monitor business activities and assess exposure to risk. Interim and year end financial statements shall be prepared in accordance with generally accepted accounting principles, as required in section 213 of the Act. The annual financial statements in all material respects shall be formatted in accordance with Part XII of Regulation 76/95.

On an annual basis, the Audit Committee will evaluate management information requirements to ensure that all information needed is regularly available and that information that was previously required and is no longer needed is terminated.

General controls will be developed to ensure that for each area of operations:

- defined authority to conduct transactions is documented
- only legal and properly authorized transactions are conducted and recorded on a timely basis

- all on balance and off balance sheet activities are accounted for, as applicable
- assets and liabilities are accurately valued
- transactions are properly classified according to the chart of accounts
- transactions are detailed in subsidiary ledgers and accurately carried forward to the general ledger.

In all operational areas (i.e., capital management, credit risk management, market risk management, structural risk management and liquidity risk management), an analysis of the risks of financial loss arising from fraud or human error, or human judgment, should be periodically conducted and appropriate, cost effective operational risk management controls should be implemented to minimize these risks of loss.

- The credit union will establish a records retention operational policy for maintaining records in order to comply with sections 230 and 232 of the Act and Part XII of Regulation 76/95, except that the period of retention of member transaction records shall be seven years rather than the statutory minimum of six.
- The credit union will develop and implement controls to protect physical assets subject to loss or misappropriation.
- The credit union will safeguard its premises, including the protection of members and staff from exposure to crime or injury.
- The credit union shall deal only with designated counterparties for material transactions.
- The credit union shall arrange adequate insurance coverage against physical property loss and shall arrange the adequate bonding of all staff and adequate indemnification insurance for directors, per board resolution.
- The credit union shall ensure that duplicates, or back-ups, of records are kept on a timely basis and held off-site.
- The credit union shall develop and maintain a disaster recovery plan. This plan shall address: staffing, communications, member servicing, facilities, hardware, software, data files, network connections documentation. The plan should be reviewed by the Audit Committee in accordance with section 26 of Regulation 76/95 and tested periodically for ongoing effectiveness.

Information Technology

The credit union will ensure that the level of technology employed adequately supports future business and strategic plans of the organization, and that it meets the requirements of generally accepted accounting principles.

New or modified systems hardware or software must be appropriately authorized and fully tested prior to going on line and will not be implemented without proper documentation and adequate training. The credit union will establish an appropriate framework for technology development. This framework will include processes for:

- identifying and evaluating technology solutions
- development and acquisition
- documentation, testing and implementation
- delivery and support.

Changes to systems must be clearly documented and tested. Adequate documentation should:

- provide sufficient information to understand the system
- facilitate supervisory review of proposed changes
- preserve continuity in the event of staff turnover
- provide auditors and others with an understanding of the system.

The Manager/Treasurer-Manager/Chief Financial Officer will ensure that adequate controls (logical and physical) are in place at all times to protect the integrity of systems, hardware, software and data.

Access to computers and file systems will be restricted to authorized personnel.

A system of passwords and other such security devices will be established and maintained to minimize the risk of unauthorized access by individuals both inside and outside the organization. This system will prescribe periodic changes to passwords. Passwords are not to be knowingly shared.

Outsourcing of Services

The credit union may outsource services by contracting a business function to a service provider instead of performing that function internally. Before this occurs, the credit union must identify:

- the process for selecting capable and reliable service providers
- standards for outsourced services, including accuracy, security, privacy and confidentiality
- procedures to monitor the performance and risks related to outsourced services and service providers
- schedules for periodic reviews of outstanding contracts.

The credit union will provide a rationale for outsourcing. Acceptable rationales include, for example, where the cost of continuing to perform the activity in-house significantly exceeds the cost of engaging an external service provider, or where the activity is of a limited or periodic nature.

Credit unions may consider outsourcing for, among other tasks:

• investment management

• information systems management

• records management

• payroll administration

• internal audit.

The credit union will complete sufficient analysis to confirm that the service provider has the necessary expertise, capacity and viability to perform the functions or activities to be outsourced. The credit union will also conduct appropriate due diligence and impact analysis of non-performance by a service provider.

All outsourced services must be subject to standard contract terms, which may include:

• the nature and scope of the service to be outsourced

• rules and limitations concerning subcontracting

• performance measures and reporting requirements

• dispute resolution and conditions surrounding defaults and termination

• ownership of information, tools, etc., and access restrictions

• audit rights

• confidentiality, privacy and security

• pricing and insurance.

The credit union's review of the service provider's performance should occur at a minimum annually, and align with the length of the contract. For example, there may be an early review three months into the term of the contract, followed by a mid-term review at six months, followed by an annual review. Each review will ensure that the outsourcing arrangement is being carried out in accordance with all contract terms and meets all contract objectives. The review should also include an assessment of the financial strength, technical competence and continuing viability of the service provider.

*** Joint stakeholder groups may be used to negotiate contracts for outsourced arrangements for a group of credit unions. The onus though, still remains with the credit union, to ensure the contract meets its criteria for outsourced arrangements.**

Reporting

Operations risk management reports provide the board with complete and accurate information concerning any material operating risk:

- outstanding overdrafts
- outstanding banking/suspense account items
- unreconciled general ledger accounts
- treasury imbalances
- internal control deficiencies
- meet the requirements of the Act and Regulations.

Compliance

Annually, the Audit Committee will ensure compliance with this policy. In accordance with section 26 of Regulation 76/95, the Audit Committee is responsible for developing and conducting an annual review of operational risk management in place (including accounting and management reporting practices), and will report its findings and recommend any necessary corrective action to the board of directors. The Audit Committee may engage the services of additional volunteers or experts to assist in their review.

The external auditor shall conduct whatever tests are necessary regarding this policy, in order to meet generally accepted auditing standards and shall report any shortfalls to the Audit Committee.

The board of directors (in conjunction with the Audit Committee, as mandated under paragraph 26.17 of Regulation 76/95) will review written correspondence from the Ministry, DICO or designated stabilization authority regarding operational risk management matters, and will investigate and respond as appropriate.

Policy Approval and Review

This policy, and any subsequent recommended changes to this policy, must be approved by the board of directors.

This policy shall be reviewed annually for ongoing appropriateness by the board (or by a delegated subcommittee of the board).