

Operational Risk Management (Internal Controls)

| Section | Topic | Page |
|---------|--|------|
| 9000 | Executive Summary..... | 9-3 |
| 9100 | Authority and Approval..... | 9-4 |
| 9200 | Safeguarding of Premises and Assets..... | 9-7 |
| 9201 | Access to Physical Premises..... | 9-8 |
| 9202 | Security Procedures..... | 9-10 |
| 9203 | Storage of Valuables..... | 9-12 |
| 9204 | Cash, Travellers' Cheques and Other Negotiable Instrument... | 9-14 |
| 9205 | Criminal Activity..... | 9-15 |
| 9206 | Safety Procedures..... | 9-17 |
| 9207 | Property and Casualty Insurance..... | 9-18 |
| 9208 | Bonding Insurance..... | 9-19 |
| 9300 | Management Information Systems (MIS)..... | 9-20 |
| 9301 | Operation of an MIS..... | 9-21 |
| 9302 | Monitoring the Accuracy of the MIS..... | 9-24 |
| 9303 | Security of MIS..... | 9-25 |
| 9304 | Disaster Recovery Planning..... | 9-27 |
| 9305 | Records Retention..... | 9-29 |
| 9306 | Records of a Permanent Nature..... | 9-30 |
| 9307 | Records to be Held Over the Long Term..... | 9-32 |
| 9308 | Records Preservation..... | 9-35 |
| 9309 | Records Destruction..... | 9-37 |
| 9400 | Staffing and Monitoring Controls..... | 9-38 |
| 9401 | Staff Supervision..... | 9-39 |
| 9402 | Segregation of Duties..... | 9-40 |
| 9403 | Hiring Staff..... | 9-41 |
| 9404 | Detecting Employee Fraud..... | 9-43 |
| 9405 | Role of Internal Audit..... | 9-44 |
| 9406 | External Auditors..... | 9-47 |
| 9407 | Audit Committee and Board Follow-up..... | 9-49 |
| 9408 | Policy Development and Review..... | 9-50 |
| 9409 | Technology Development..... | 9-41 |
| 9410 | Outsourcing of Services..... | 9-42 |

Executive Summary

The board should establish an operational risk management policy that sets includes the requirements, purpose and scope of related internal controls. Management should document internal controls in the credit union's operational procedures. Documentation assists in ensuring that internal controls are properly authorized and complete, and assists in their maintenance and revision.

Operational risk management includes implementing:

- defined levels of authority to make corporate decisions;
- safeguards to protect the premises and assets of the credit union;
- an operational and secure management information system (MIS) which accurately records transactions;
- staffing and monitoring controls appropriate to the size of the credit union;
- a framework for technology development
- a process for outsourcing services
- appropriate monitoring controls.

The specific elements of a comprehensive internal controls system are set out in DICO's By-law No. 5. Internal controls relating to credit granting practices are covered in Chapter 5 on Credit Management.

In designing a system of internal controls, management must review the costs and benefits of implementation. The cost of establishing a particular control must be measured against the expected savings attributable to loss prevention (e.g. reduction of fraud). A particular internal control may not be required where in its absence the likelihood of financial loss is small due to the size of the operations or the existence of compensating controls.

A credit union can meet the standards of sound business and financial practices by ensuring it has developed and implemented policies and procedures comparable to those contained in this chapter. Policies and procedures should be appropriate for the size and complexity of operations.

Authority and Approval

A primary factor of operational risk management is the existence of a framework of defined levels of authority to make corporate decisions. Management must design and implement a framework for approval authorities, for all areas of operations which ensures that responsibilities and approvals for transactions are assigned to the proper and appropriate individuals within the organization.

The following essential elements of an approval framework should be required by board policy, and should be documented in internal control procedures:

- General approvals;
- Specific approvals;
- Designated signing authority;
- Organizational chart;
- Designated suppliers of professional services.

General Approvals

General approvals need to be set within the procedures and job descriptions, for a group or class of transactions. They should provide staff with the authority to complete a transaction without receiving specific approval.

Specific Approvals

Specific approvals are those that will require an authorizing action, evidenced by signature, before the transaction can be completed. Specific approval authorities document:

- 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.

Signing Authority

The approvals framework should govern the signing authority of credit union's officers and management. The framework should address signing of:

- corporate cheques;
- documents under seal (e.g. mortgage discharges);
- all contracts accepted on behalf of the credit union.

Cheques over a prescribed dollar amount should require signatures by two officers, or at least one officer and one staff member.

Authority to Enter into Contracts

Internal controls should provide for the following safeguards when officers or staff enter into the contracts on behalf of the credit union:

- Contracts which are entered into should comply with legislated requirements and the objects of the credit union.

- Where the approval of a contract results in a conflict of interest for a director or officer, the individuals involved must be guided by sections 146 to 149 of the Act, as well as legislation on restricted party transactions, in Part IX of the Act and Part X of Regulation 76/95. (Refer to Section 2104 for further details in this regard.)
- Contracts over a specified dollar amount should be subject to the control of dual, independent signatories. The specified amount should be determined by the board in relation to the organization's asset size and transaction base.
- Contracts which commit the organization to external borrowings must be subject first to board approval, and then require the manager and other senior officers' signature for validation.
- Smaller purchases or contracts which commit the organization to daily business activities should have the signature of one or more operating officers and should be in compliance with the credit union's capital budget, as approved by the board.
- With respect to the authorization of loan contracts between the organization and its members, refer to Section 5502 of this Reference Manual on Loan Approvals and Disbursements.
- Investment contracts should be authorized in compliance with a documented board policy on investments. Refer to Section 6204 of this Reference Manual on Investment Approvals.

Organizational Chart

An organizational chart illustrates lines of reporting, responsibility and authority between staff, and is a useful tool in representing the authority framework of the credit union.

Designated List of Professional Service Suppliers

The credit union should specify in policy or procedures designated suppliers of professional services. The purpose of this process is to ensure that the credit union retains professionals whose credentials and qualifications have been investigated.

This can be ensured by requiring such investigation before a professional can be added to the designated list, and by limiting the credit union to only retaining professionals from that list. Investigation should ensure that professionals have the proper qualifications and insurance. Operational procedure (or policy) should specify the process for adding qualified professionals to the list.

Professional services which should be covered in the list include:

- legal counsel;
- real estate appraisers;
- financial advisors (brokers, investment dealers, and other financial service providers).

A review of internal controls at the end of the year should include a check to ensure only professionals from the designated list were retained by the credit union.

Safeguarding of Premises and Assets

The safeguarding of premises from theft, burglary, robbery and other physically hazardous conditions which may cause harm to staff, members, or general property should be a key objective of policy. In order to reduce the risk of such acts being committed against the credit union, four basic areas of risk management are recommended:

- Access to the credit union's property should be monitored and subject to certain physical controls.
- Storage of valuables must be strictly regulated and protected in fire and theft resistant receptacles (e.g. safes, vaults, etc.).
- Security procedures should be defined and followed by staff.
- Insurance coverage should be utilized to reduce the risk of monetary loss from accidents.

The extent of protection and the degree of precaution which must be implemented under each of these categories will vary amongst credit unions, and should be determined based on:

- the incidence of crimes against the particular office or financial institutions in the area in which the office is located;
- the amount of moneys, securities or other negotiables exposed to robbery, burglary, or theft;
- the distance of the office from the nearest law enforcement offices, guards, or security personnel and the time required for such personnel to arrive at the office;
- other security measures in effect at the office or within the area, such as the office being located within the complex of a business or factory which has security, etc.;
- the physical characteristics of the office structure and its surroundings.

Detailed recommendations on these categories of risk prevention for physical premises and assets follow.

Access to Physical Premises

It is recommended that at a minimum the following security equipment be installed to deter unauthorized access to the premises of the credit union.

- A lighting system must be in place which effectively illuminates all areas surrounding exterior entrances to the premises, including the parking lot and any automated banking machines.
- Minimal lighting of the interior office should be provided after hours, and curtains should be left open to permit police and/or security personnel to detect illegal entry.
- The vault or safe door should be visible from outside the office if possible to promote direct surveillance by the public and the police.
- Where public resources are available, arrangements could be made with local police or other security personnel to inspect the exterior of the premises with reasonable frequency.
- Emergency lighting (and alarm) facilities must be equipped with an independent source of power, such as a battery, in the event of failure of the usual source of power.
- Tamper resistant locks should be installed on exterior doors and windows. Rear and/or basement windows should be protected by burglary resistant bars or grills. It is recommended that all outer door locks have dead-bolts with keys that are registered and cannot be cut by ordinary locksmiths without written authority.
- Keys to the premises, the vault/safe or other safekeeping drawers must be maintained under a strictly applied policy of key control. An inventory of all keys should be prepared, listing the authorized personnel to whom they have been assigned during the day.
- Underwriter Laboratories of Canada (ULC) certified alarms should be installed on all safes/vaults. In addition, premises alarms can be installed for peripheral safety (e.g. motion detectors). The alarm system should provide for employee (e.g. teller) activation after a robbery, preferably a silent activator, that is connected to the police or a security agent. The equipment should have a visual and audible signal capable of indicating improper functioning or tampering with the system.
- A camera surveillance system should be installed, where practicable, to monitor all entrances, tellers' counters, ATM areas and vault access. Notice of the existence of such devices should be prominently displayed and surveillance equipment continuously supplied with new tape or film as required.
- Customers and other members of the public should be kept away from rooms or areas that are not used to serve the public.
- ATM facilities should be established in well lit areas, preferably near paths of public traffic for surveillance purposes.
- Where a staffed drive-through teller window is used by a credit union to service members, the window should have bullet proof glass installed. The teller in a drive-through teller window should be protected by a robbery alarm activator and video/camera surveillance.
- Local police should be consulted in designing an effective program of crime prevention.

Security Procedures

The existence and enforcement of routine policies and procedures for the opening and closing of premises is another important element of risk management. The general manager, or other officer responsible for internal controls, should devise and oversee implementation of these practices at the credit union.

Where a perimeter alarm and motion detector is not in place, the following practices are recommended for the opening of premises:

- Specific senior employees should be designated to open the office or the branch on a daily basis. Employees should enter the premises through the front or main entrance doors, paying attention to suspicious persons who may be loitering near the office. When in doubt, police should be notified.
- At least two persons should be present during the office opening. One person should remain outside the office while the other(s) inspects the interior premises, and gives clearance to exterior staff for entry. When clearance is not given within a reasonable time, the staff outside should contact the police from an outside location.
- If there is only one employee, he/she should telephone a responsible person by a specified time, advising that everything is in order using a code word.
- If upon entry, a break-in is discovered, staff should evacuate the premises, and call police from an outside location. Caution should be used so that fingerprints or other evidence is not destroyed.

Specific senior employees should be assigned to close the branch or office each night. The following safety procedures are recommended:

- All doors and windows must be locked and checked thoroughly for damage and improper locking mechanism. Rooms, closets and basement should be inspected to ensure unauthorized persons have left the building.
- Cash drawers and anti-hold-up units should be left empty and should remain open with keys removed. The cheque protector, certified cheque and other stamps should be locked away.
- All securities and records should be stored in appropriate containers and locked; wastebaskets should not contain confidential data.
- Combinations on teller lockers should be spun off. The vault/safe should be locked and all security and alarm devices should be checked to ensure these are activated.

Once the office is closed for the evening, it is strongly recommended that individual staff not remain behind after hours. Where it is necessary to do so, two persons should be in attendance. The alarm company should be notified that staff are still on the premises so that employees are not mistaken as intruders.

Storage of Valuables

It is recommended that suitable storage units be used to protect the valuables of the credit union from theft or destruction. Refer to Schedule 9.1 below for a list of recommended equipment.

| Schedule 9.1 STORAGE OF VALUABLES | |
|--|---|
| Type of Valuable | Recommended Storage Unit |
| Teller Cash | Teller drawers, drop safes and anti hold-up units |
| Cash In Transit | Night depositories and armoured vehicles |
| Surplus Cash and Negotiable Securities | ULC certified vault or safe with a time lock and delayed action timer |
| Member Personal Valuables | Safety deposit boxes |
| Member Records | Fire resistant storage cabinets |
| Loan Security Documents | ULC certified vault or safe |

- Burglary ratings for all safes and vaults should be investigated with a league, or the bonding insurance company; equipment purchases must be in compliance with the requirements for bonding purposes.
- A written certificate from the contractor, manufacturer or supplier of the equipment should be obtained, documenting that the equipment meets or exceeds recommended qualifications.
- All key and combination locks which are installed on storage units should also be in compliance with recommendations made by a league or the bond insurer.
- It is strongly recommended that all vault combinations have time delay mechanisms which require pre-setting for daily operations, and require two combinations to open.
- A record of all combinations for combination locks should be kept in safekeeping, under dual custody preferably off premises. Combinations should be changed at least annually, after servicing or whenever there is staff turnover.
- All storage devices should be regularly inspected, tested (e.g. at least annually) and serviced by competent persons to assure maximum performance and safety. A record should be kept of all inspections and servicing.
- A perpetual inventory list of all equipment and fixed assets owned by the credit union should also be maintained.

Cash, Travelers' Cheques and Other Negotiable Instruments

Cash, travelers' cheques and other negotiable instruments represent a significant portion of the stored assets of a financial institution. As a result, this area warrants special focus. The following general internal controls are recommended:

- Cash and negotiable securities must never be left unguarded when outside of the vault, and should be secured at all times.
- Where possible, dual control of negotiables by independent persons should be exercised, meaning that at least two staff members should be required to access valuable property.
- Where single control of cash and negotiable instruments is required for operational expediency, (e.g. a teller's control of his/her cash drawer) the property which is entrusted to a single employee should be counted.
- Controls should be in place to log all transactions while funds are entrusted to an employee. When cash is returned to treasury or to another employee, it should be counted by the persons responsible for treasury.
- Procedures should exist for establishing the accountability of cash shortages. Tellers should be required to balance their cash at the end of their shift.
- Detailed internal control procedures for the handling of cash should be documented by the credit union, and must be distributed to all staff who handle funds.

Internal controls may also be necessary to provide proper safeguards for cash, cheques, and negotiables located in:

- tellers' drawers;
- treasury;
- transit;
- night boxes and ATMs;
- safety deposit boxes.

Criminal Activity

Internal controls must address the threat of criminal activities from both within and outside the credit union. While the indemnification of losses from most criminal activities is provided for by mandatory bonding insurance, strategies are needed to minimize the likelihood and the effects of these activities, in order to protect members and employees from harm, and to keep bonding insurance premiums to a minimum. Refer to Schedule 9.2 for a sample list of criminal activities which should be addressed by internal control policy and procedures. A credit union can contact its league for assistance in setting up these procedures. One of the more common forms of criminal activity, money laundering is discussed below in greater detail.

| Schedule 9.2 COMMON CRIMINAL ACTIVITIES FACING CREDIT UNIONS |
|---|
| <ul style="list-style-type: none">• Bomb threats• Extortionist telephone calls• Kidnapping of employees• Robbery• Burglary• Embezzlement• Mysterious disappearance• Forgery• Money laundering• Cheque kiting |

Approaches to managing associated media publicity that results from detected criminal activities should also be incorporated into these procedures.

Money Laundering

Money laundering is defined as a criminal process whereby the existence of an illegal source, or illegal application of income is concealed by the re-circulation (laundering) of that income through legal deposit taking institutions. Money laundering makes illegal cash appear legitimate. Generally the process is accomplished by individuals depositing illegal cash into a variety of accounts, in periodic instalments that do not arouse suspicion. The deposit of illegal proceeds into a financial institution is often accompanied by the practice of frequent cash transfers by wire or other methods, the conversion of cash into money orders, travelers' cheques, precious metals or other negotiable instruments, or the frequent changing of currency into different denominations of cash. Under Canada's Criminal Code, it is a criminal offence for anyone, including credit union staff, to knowingly assist in laundering the proceeds of crime.

Credit union staff should be advised of the likely indicators of money laundering and should be trained to be suspicious of transactions that do not appear legitimate. It is recommended that the following unusual member behaviour be documented by tellers or service representatives, and communicated to the general manager, controller or internal auditor:

- Unusually high and frequent cash deposits made by a member in person, by automated teller or night depository, usually followed by transfers clearing the account.
- Irregular large cash deposits or withdrawals made by a business that seem unreasonable for the nature of the enterprise or which would normally be dominated by cheques or other instruments.
- Members which decline or provide minimal information for new accounts or for other banking services which would be valuable to them.
- Members which frequently seek to exchange small denomination bills for larger ones, or whose deposits contain counterfeit bills.

In general, credit union general managers and staff should be familiar their members and their sources of funds, while at the same time noting and questioning any suspicious transactions. Where criminal activity is suspected, supervisory staff should transfer any evidence to the Risk Management personnel of the appropriate league, bonding agency or to police.

Management and staff must also be aware of and comply with the federal regulations on money laundering. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires the credit union to implement a compliance regime for identifying and reporting certain large and suspicious transactions.

This includes:

- the appointment of a Compliance Officer (for each branch location)
- development, approval and application of written compliance policies and procedures
- implementation of an ongoing employee compliance training program
- a regularly scheduled review of policies and procedures by internal/external auditors to test their effectiveness, adopt changes in legislation and correct any weaknesses

Further information is available directly from FINTRAC (Web site <http://www.fintrac.gc.ca>), your league or Credit Union Central of Canada.

Safety Procedures

Steps should be taken by the credit union to conduct routine safety inspections of all office property, property in possession and foreclosed real property. The following guidelines are recommended:

- The credit union should at least annually inspect fire prevention equipment including office sprinklers and fire extinguishers.
- The need for installation of fire walls should be considered where the credit union's office is adjacent to fire hazardous occupants in the same building (e.g. restaurants, laundries, etc.).
- Employees should be trained in fire prevention, and regular fire drills should be conducted. The local fire department should be consulted in establishing a fire prevention program.
- All heating and electrical equipment should be routinely inspected to prevent performance failures and/or explosions.
- Elevator shafts and vents within a building should be kept free of trash, dust and other combustible materials.
- Waste should always be stored in enclosed metal containers, away from heating sources.
- Entrances, stairways, office aisles and loading platforms should be kept unobstructed by trash or storage boxes.
- Floors should be clean and dry to prevent accidental slippage.
- Outside areas such as parking lots and sidewalks must be cleaned of snow and ice, and must be brightly lit at night. Walkways and steps should be in good repair.
- Office equipment should be sturdy and safe for employee use. Large, clear plate glass windows should be marked at eye level, and not located where persons can accidentally walk through them.
- Where the office is situated in an industrial plant, management should ensure hazardous industrial materials are not located close to the office.

Property and Casualty Insurance

Adequate property and casualty insurance should be obtained by each credit union from a general insurer. The extent of coverage must be assessed relative to the original and replacement costs of insured property.

The purpose of property and casualty insurance is to safeguard the organization against damages caused by accidental occurrences such as the following:

- Fire and similar damages - arising out of fires caused by lightning and explosion, smoke, water, chemical, etc.
- Weather and other perils - such as hail, windstorm, explosion without fire, vandalism, etc.
- Automobile accidents - for both owned and non-owned automobiles.
- Theft - including larceny, robbery and burglary.
- General liability - arising out of injury to persons entering upon the premises.

Bonding Insurance

In accordance with section 151 of the Act, bonding insurance for officers and staff must be obtained.

The prescribed minimum amount of coverage is set out in section 27 of Regulation 76/95. The coverage that is provided by a fidelity bond should include indemnification for losses caused by counterfeit money or securities, robbery, burglary, theft, forgery, or employee/director/committee member dishonesty.

Although a regulatory minimum is prescribed in Regulation 76/95, the board of directors still need to review the amount of bonding insurance coverage held by the credit union to determine if it is sufficient given the credit union's operations. Increased coverage, even that greater than the regulatory minimum, should be obtained if necessary to provide sufficient protection for the credit union.

Certain maximum limits and exclusions for liability are specified in the insurance agreement which should be fully reviewed. Management should be aware of these.

Credit unions not covered through a league master bond program must obtain bonding insurance directly from the insurance company. Bondability of an employee is a requirement of bonding insurance, and therefore the credit union must ensure that all current staff are bondable.

Similarly, any new staff must be bondable as well. Details of procedures for bonding new staff members can be obtained from the insurance company, or from the league if it institutes a master bond program.

Management Information Systems (MIS)

The board shall establish a policy that will address the operation and security of a management information system (MIS). The objectives of an MIS is to provide timely and accurate processing of authorized transactions in a controlled manner and to produce informative monitoring reports for management purposes. It is therefore recommended that policy require the following:

- the accurate operation and security of a management information system, which:
 - records all transactions accurately and on a timely basis;
 - enables management to monitor and analyze the financial condition and performance of the credit union;
 - provides an audit trail for all transactions;
 - protects the integrity of system hardware, software and data through appropriate access and process controls
 - addresses the audit and regulatory record retention requirements of the organization;
- a Disaster Recovery Plan that can respond to situations of severe damage to the physical premises or computer system of the credit union (including data back up);
- a system of record retention, storage and destruction.

These elements are discussed in Sections 9301 to 9309 of this chapter.

Operation of an MIS

A management information system (whether manual or electronic) should be designed to collect relevant data on a timely basis and to generate reports which satisfy management's decision making requirements, as well as the board's monitoring function. Financial data collection should permit management to:

- prepare financial records and books of account;
- monitor and analyze the credit union's financial condition and performance (including determining and explaining financial trends);
- compare key financial ratios to targets in the annual business plan, historic performance and peer/industry performance;
- satisfy regulatory requirements, such as monitoring compliance with the Act and Regulations, and record retention.

Accounting Records

The MIS should include a set of accounts, general and subsidiary ledgers and a prescribed flow of standardized documents which will record accurately the effect of all economic transactions on each financial statement component. The MIS should maintain the following records for each main office or branch of a credit union:

- General ledger control accounts which provide a summary record of all the transactions which affect the assets, liabilities, income, expenses and equity of the credit union.
- Schedules for the support of balances in general ledger accounts including:
 - allowance for doubtful loans;
 - depreciation schedules;
 - monthly bank reconciliation;
 - investments schedules;
 - other such schedules as may be required.
- Subsidiary ledger records for all member accounts, in balance with their respective general ledger control accounts including the following:
 - individual loan accounts (including personal, mortgage, commercial, etc.);
 - individual chequing accounts;
 - other individual deposit accounts (savings, RRSP, term deposits, etc.);
 - individual share accounts;
 - individual loans that have been written off;
 - other such individual subsidiary ledgers as are necessary to account for and support a general ledger account.

Note: Subsidiary ledger accounts should be reconciled to general ledger accounts by someone who is not involved in making transactions to either ledger, and checked by a supervisor.

- An "inter-branch" general ledger account for the recording of the net shifting of funds between branches, where applicable.

Where a credit union has branch operations (i.e. branches permitting member sign-up and the completion of loan applications), it is recommended that the records of each branch be maintained separately in order to monitor the branch's business volume, costs and revenues of operation. Account numbering across branches should be standardized with individual branch codes identified.

Where the branch operation is part of an interactive data processing system, accounting transactions should be recorded, where initiated, in separate branch controls for branch information purposes. All transactions should also be consolidated in a central control account for head office monitoring.

Reports

Each credit union must develop a policy on what management reports shall be produced by the system and to whom these reports shall be distributed. Refer to Chapter 1 on Risk Measurement and Reporting for financial information recommended to be prepared and reviewed on a periodic basis by the board.

At a minimum, each main office or branch of a credit union (where feasible) should produce monthly accounting reports which include:

- a balance sheet;
- a statement of income;
- supporting financial statement schedules (e.g. allowance for doubtful loans);
- loan activity report;
- statistical reports for regulatory purposes.

Where there are branches in operation, a consolidated financial report of all branch reports (including a consolidated loan activity report) should also be prepared by head office. In this report the inter-branch control account must be equal to the sum total of all "inter-branch" general ledger accounts.

Risk and Performance Measurement

The MIS should also enable management to measure actual performance and business risk, and report the results of these measurements to the board, as required in DICO By-law No. 5.

The results of these measurements must be reported on a periodic basis to the board, either in one comprehensive report, or by operational area, as detailed in Schedule 9.3.

| Schedule 9.3 | |
|--|-----------------------------------|
| BOARD REPORTING ON RISK AND PERFORMANCE MEASUREMENT | |
| Report by Operational Area | Frequency of Board Reports |
| Capital board report | every board meeting |
| Credit board report | monthly |
| Investments board report | every board meeting |
| Asset/liability management board report | at least quarterly |
| Liquidity board report | every board meeting |
| Internal Controls board report | at least quarterly |

Monitoring the Accuracy of the MIS

The MIS, whether manual or electronic, must be efficient and reliable, generating a minimal number of errors. The following procedures can assist to ensure the accuracy of the MIS:

- A log of processing mistakes should be maintained and reviewed by management to analyze and correct system errors.
- A management review of system design and capacity should be performed at least annually, for the purpose of identifying required improvements.

These procedures should be practical and reasonable given the size and complexity of the MIS. The more sophisticated the system, the greater the availability of reports to detect system bugs, errors and possible fraud. Schedules 9.4 lists some sample transaction edit reports and system activity reports for this purpose.

| <i>Schedule 9.4</i> <i>TRANSACTION EDIT REPORTS AND SYSTEM ACTIVITY REPORTS</i> |
|---|
| <p>Transaction Edit Reports</p> <ul style="list-style-type: none">• Loan payments report• Loan disbursements report (records all new loans)• Loan status report (records override adjustments to terms and conditions of member loans)• Deposit master file report (records changes to interest rates, interest recipients)• Large debits report (records deposit withdrawals over a certain size)• General ledger activity report• Dormant account activity report• Suspense account activity report• NSF and stop payment report <p>System Activity Reports</p> <ul style="list-style-type: none">• System console log (e.g. log of all system activity including inquiries)• Job runs processed by the computer (most software for P.C. based systems have a job logging facility)• Data error reports• Operator job interventions (e.g. system overrides)• Terminal user password violation attempts• Terminal restriction violation attempts• Report of files updated (e.g. loan master file changes)• Report of file status (e.g. file is full)• Daily schedule of reports issued by the system |

Security of MIS

Computerized facilities that are used to record monetary transactions of members and/or general ledger activities of the credit union must be adequately protected, whether the equipment has been provided through a service bureau or it is an in-house system.

Schedule 9.5 summarizes the basic type of controls that should be used to protect the security and accuracy of a computer system. The most important of these controls is the frequent creation of back-up files for transactions and financial data, and storage of the back-up data at an off-site location.

| Schedule 9.5 | |
|--|--|
| COMPUTER RISK MANAGEMENT | |
| Internal Controls | Protects Against: |
| Equipment safeguarding <ul style="list-style-type: none"> • Restricted access computer area • System maintenance • Disaster planning | <ul style="list-style-type: none"> • Theft and vandalism • Equipment failure • Loss of data during natural disasters or fires |
| File storage controls <ul style="list-style-type: none"> • File library • Off site back up of files • Record destruction policy | <ul style="list-style-type: none"> • File mislabeling • File destruction • Permanent loss of information |
| File access controls <ul style="list-style-type: none"> • File access codes (passwords) • File activity logs • Data encryption | <ul style="list-style-type: none"> • Unauthorized data tampering or monitoring |
| Organizational controls <ul style="list-style-type: none"> • Program design and testing • Staff training and supervision • Segregation of duties | <ul style="list-style-type: none"> • Poor management reports • Untimely processing |
| Data input/output controls <ul style="list-style-type: none"> • Error logs • System edit checks • Controlled source documents • Management review of output | <ul style="list-style-type: none"> • Inaccurate data processing • Unauthorized data processing |
| Documentation <ul style="list-style-type: none"> • Documentation of all software • Log kept of all software updates • Changes to software documented | <ul style="list-style-type: none"> • deterioration in business relations with data suppliers • data supplier goes out of business |
| Web sites and Internet Banking <ul style="list-style-type: none"> • Safeguards • Firewall security | <ul style="list-style-type: none"> • unauthorized access • fraud |

Disaster Recovery Planning

It is a sound business practice for the credit union to have a disaster recovery plan. A disaster recovery plan is a contingency plan for the recovery of data processing facilities, and for the protection of financial data caused by short, medium and long-term system interruptions.

The disaster recovery plan should outline in detail the alternate procedures to be followed during system interruptions. Procedures should be tested periodically to ensure they are operable and that staff are aware of their implementation. The plan should be managed by a designated senior member of staff who functions as a disaster recovery controller and should be reviewed by the credit union's audit committee (section 26.12 of Regulation 76/95).

Recovery plans should be documented and include the following:

- The board policy which commits the organization to disaster planning.
- Emergency reaction and disaster control steps which must be taken immediately.
- Identification of the back-up location where data processing operations will continue
- Back-up data processing facilities or agreement with data supplier to provide new equipment within 24 hour period.
- A step by step action plan for each department or functional unit of the credit union to return operations to normal.

Adequate insurance coverage should include business interruption, the cost of data reconstruction and/or lost data, as well as alternate processing capacity. Refer to Schedule 9.6 for a summary checklist on disaster planning.

| Schedule 9.6 DISASTER RECOVERY CRITICAL PATH |
|---|
| <p>Emergency Reaction Steps</p> <ul style="list-style-type: none">• Detection and notification of emergency to:<ul style="list-style-type: none">○ Fire department○ Police department○ Hospitals○ Utilities• Evacuation procedures• Clear and secure site• Minimize loss of life, property, business interruption <p>Disaster Control Steps</p> <ul style="list-style-type: none">• Control access to site• Consider and evaluate staff requirements during the disaster• Activate back up facilities or obtain new equipment for immediate processing• Assess damages and make insurance claims• Co-ordinate clean up• Co-ordinate press communications <p>Business Survival Steps</p> <ul style="list-style-type: none">• Establish telecommunication links, cash, courier and mail deliveries to a back up site• Re-establish office conditions on a full or limited basis by leasing office equipment• Communicate with suppliers and staff on new arrangements• Arrange for adequate security at new site (e.g. fire and theft alarms, temporary vault, security guards)• Implement public relations plan for members and the public• Manage and prioritize key profit areas <p>Reconstruction Steps</p> <ul style="list-style-type: none">• Employ contractors and restoration companies for refurbishing office as may be required• Reconstruct records• Return operations to normal• Document and evaluate experience of what happened |

Records Retention

The operational records of a credit union provide important evidence of its business activities. These records may be called upon by regulators, tax authorities, members, employees, auditors and lawyers in a variety of circumstances. A procedure on records retention, specifying which records should be retained, for how long, and in what form, is required.

The procedure must accommodate various reporting obligations imposed by statute, including:

- the *Credit Unions and Caisses Populaires Act*;
- the *Income Tax Act*;
- the *Unemployment Insurance Act*;
- the *Canada Pension Plan Act*.

Other acts such as the Canada Evidence Act, the Evidence Act of Ontario and the Statute of Limitations create additional implications for the nature and timing of record retention. Certain documents must be retained for as long as the credit union is in operation; others may be destroyed after a specified time interval.

The procedure on records retention should include a Schedule of Records Retention, which specifies the types of documents that must be retained, in what fashion, and for how long. This schedule should be copied and distributed to all personnel handling member and financial documents. The procedure should be reviewed periodically for its continued applicability.

The disposal of outdated records and the transfer of inactive files to archives should take place at least once a year, most preferably after the fiscal year end and audited financial statements have been completed.

The following materials provide detailed recommendations on record retention.

Records of a Permanent Nature

Sections 230 and 231 of the Act specify that certain corporate documents be retained on a permanent basis, that is for as long as a credit union is in operation. The following is a list of the records which should be considered permanent, and must be retained:

- Share register (e.g. share ledger account) which includes the names and addresses of members, the number of shares held, the date of registration and the dates on which persons ceased to be members (s. 230 of the Act).
- Articles of incorporation (s. 231(1) of the Act).
- By-laws, including all subsequent resolutions and special resolutions (s. 231(1) of the Act).
- Register of the names, addresses, occupations and terms of office for members of the board of directors, the credit committee, the supervisory committee and audit committee (s. 231(1) of the Act).
- Register of all securities held by the credit union (s. 231(1) of the Act).
- Books of account and accounting records detailing all financial and other transactions of the credit union as required by the Superintendent of Financial Services (s. 231(1) of the Act).
- Minutes of all meetings of the members, the board of directors, and any committees (s. 231(1) of the Act).

Section 232 specifies the form for which a record may be kept for purposes of the Act. The section allows for keeping records in forms other than their original (e.g. photocopies, microfiche).

Other acts such as the Income Tax Act, the Trustee Act and the Winding Up Act also require documents to be kept permanently. The following is a list of such documents, as well as other documents which it is recommended that the credit union should retain permanently:

- Certificates and permits to operate in Ontario or outside the province.
- Deeds, titles, abstracts, collateral documents to land, buildings, and equipment.
- Records recording insurable members' savings accounts.
- Audited financial statements (including a balance sheet, a statement of operations, a statement of undivided earnings, and a statement of reserves and any other financial information the by-laws require).
- Special agreements or contracts mentioned in the audited financial statements.
- Reports of the auditor.
- Official correspondence of a permanent nature received from the Superintendent of Financial Services and other government sources.
- Official correspondence received from DICO (e.g. DICO By-laws).
- Technical bulletins received from the league.
- Records destruction list detailing which documents have been destroyed.

Insurable Members' Savings Account

Many credit unions offer a life insurance policy on members' shares or other savings accounts with insurable values based on the date of deposit. These records should be retained for an indefinite period of time after a members' death to handle subsequent inquiries regarding settlement.

Records to be Held Over the Long Term

Tax Supporting Documents

The *Income Tax Act* and the *Statute of Limitations* have pervasive implications for long term records retention by the credit union. From the perspective of the income tax authorities, documents (other than those designated as permanent records) may be destroyed without permission six years after the end of the taxation year to which the books and records relate. In order to be conservative, it is recommended that credit unions retain these records for a period of seven years.

Refer to Schedule 9.7 for a list of accounting data and other source documents pertaining to members' transactions which should be retained (also refer to section 95 of Regulation 76/95).

| <i>Schedule 9.7</i> <i>DOCUMENTS QUALIFYING FOR SEVEN YEAR RETENTION</i> |
|--|
| <p>Accounting Data</p> <ul style="list-style-type: none"> • General ledger, cash journals, audited financial statements • Loans subsidiary ledger • Deposits subsidiary ledger • Employee payroll subsidiary ledger and employee expense records • Bank statements, returned cheques, deposit and debit slips of the credit union • Clearing reports • Supplier invoices/expenses statements • Periodic financial reports (e.g. budget to actual comparisons) <p>Members' Account Data</p> <ul style="list-style-type: none"> • Account operating agreements and signature cards following closure of an account • Debit/credit memos • Copies of members' statements • Microfilmed members' cheques (generally retained by clearing agent) • Members' deposit/withdrawal slips and transfer vouchers • Term deposit certificates with members • Loan files containing loan applications, details of loan analysis, client correspondence and any collection action • All memoranda received or created concerning account operation |

Records that support the calculation of other taxes such as sales tax, withholding taxes etc., and all payroll deductions such as unemployment insurance, Canada Pension Plan etc., must also be retained for six years from the end of the taxation year to which they relate for possible government inspection.

The contents of documents and books of account which must be archived for tax purposes have not been specifically defined by the tax authorities; the general guideline is that records retained must substantiate the determination of tax liability, and must be supported by vouchers or source

documents. The six year retention period applicable to a document that supports a tax liability is determined by the last taxation year that the record was used for the calculation of tax, and not the year that the underlying transaction occurred or the year the record was created.

Books of Account

Books of account must be maintained in an orderly manner at the premises of the credit union, and must be made available to income tax authorities for review purposes at any reasonable time.

Revenue Canada recognizes as acceptable the following methods of keeping records:

- traditional books of account;
- records maintained in a machine sensible data medium which can be read by current hardware equipment and which can be related back to supporting source documents;
- microfilm reproductions of books of account and source documents if produced under a microfilm program which conforms with Revenue Canada's standards.

Defending against Legal Action

The possibility of a credit union becoming involved in a legal action provides additional rationale for members' source documents to be retained on a long term basis (e.g. documentation of a loan write-off). A record should only be destroyed once the credit union ascertains that the document is not and cannot become an essential link in defending or prosecuting a court action.

Mergers

In the event that a credit union merges with another, the permanent records of the acquired credit union should be considered the permanent records of the continuing credit union, and should be maintained under the same standard of care.

Dormant Accounts

Dormant accounts should be reviewed annually for the purpose of confirming future account liability. Balances in dormant accounts should be communicated to members by mail.

It is suggested that at a minimum:

| | |
|--|--|
| After two years without any customer initiated activity | ▪ Forward notice to the member's last known address |
| After five years without any customer initiated activity | ▪ Forward notice to the member's last known address ▪ Transfer funds to "Unclaimed Balances" (general ledger) account |

The accessing of dormant accounts by unauthorized personal or by staff is also a specific area of risk which should be addressed and subject to controls. Once an account is designated as "dormant", any deposits and withdrawals should require supervisory authorization. Authorization to "reactivate" a dormant account should require the signatures of two employees, one of who is a supervisor.

Note: Section 45 of the Credit Union and Caisses Populaires Act, 1994 has not been proclaimed.

Accordingly, there is currently no requirement to forward unclaimed credits to the Ministry of Finance.

Operational Records

With respect to operational records, other than books of account and members' transaction documents discussed earlier, credit unions must adopt guidelines for archiving records of historical significance, i.e. operating files which have become inactive but support important internal decisions taken by senior management (e.g. product/branch/human resource decisions). A retention period of five to six years is recommended for these documents; however, the retention period for these records is entirely at the discretion of management. Duplicate copies in the hands of other users may be destroyed earlier. Refer to Schedule 9.8 for a sample retention schedule for operational records of historic significance.

| Schedule 9.8 OPERATIONAL DOCUMENTS OF A HISTORIC SIGNIFICANCE ELIGIBLE FOR LONG TERM RETENTION |
|--|
| <ul style="list-style-type: none">• Planning documentation (directional plan, strategic plan, budgets)• Policies and procedures• Employee files including performance reviews• Product analysis• System studies• Marketing surveys• Cost/benefit analysis and regulatory compliance analysis for investment decisions• Official league correspondence (e.g. operational or loan reviews)• Public relations activities• On-site verification reports, auditor's reports and auditor's management letters |

Records Preservation

The following are recommendations for the general storage of documents:

- Ensure records are protected from fire, smoke, heat, water, dirt, and accidental and malicious damage.
- Store accounting and members' transaction records in a vault, safe or fire resistant cabinet when not in use.
- Make duplicate copies of computer disks, computer tapes and microfilm and store them separately from the originals in fire proof receptacles, or at another site.
- Ensure the credit union's insurance program includes "business interruption" coverage or an "extra expense" policy that will cover the cost of recovering or replacing records that have been damaged or destroyed.
- Where a credit union uses a service bureau to process its data, confirm that the service bureau is bonded and the company is reputable, to ensure the confidentiality of records.
- Consider using a commercial service to microfilm and/or store records; where reliance is placed on external agents for these functions, sufficient investigation must be made into the quality and reliability of such services.

Storage of Vital Records

Credits unions are advised to develop a procedure on the storage of vital records. Vital records are defined as those records which are necessary to re-establish operations after a disaster. These would include documents such as the general ledger, tax records, investment contracts, employee records, and up-to-date balances of members' deposits and loans.

The procedure must ensure that duplicates of vital information be stored off-premises in the event that a disaster occurs and the original records are destroyed. This procedure can be developed in conjunction with, or as part of, the Disaster Recovery Plan.

The following information, at minimum, should be copied and transferred regularly to an off-site storage location:

- A listing of the members' share and/or deposit and loan balances as of the record date by individual account number.
- A financial report which includes a list of all asset and liability accounts as of the record date.
- Names and addresses of the credit union's deposit holding institutions and clearing agent, location of safety-deposit boxes and other places where records are stored.
- List of insurance policies such as fire, casualty, life savings and borrowers' protection, fidelity bond, etc. with the names and addresses of the insurers.
- A detailed listing of all investments.
- Up-to-date documentation of the credit union's in-house computer system.

Manual tape listings, copies of original manual records, computerized reports, magnetic tape or microfilm are all considered acceptable forms of documentation in this regard.

Records Destruction

With the exception of records that must be retained permanently (listed above), corporate documents should be scheduled for disposal in a systematic manner, in accordance with board policy, internal controls procedures, and an approved Schedule of Records Retention. The major objective of systematic records disposal is to ensure effective and efficient use of space, material and staff in the management of records.

The following guidelines regarding destruction of records is recommended:

- Consider retaining paper waste for a minimum number of days before destruction, in order to find teller differences or important lost documents.
- If feasible, dispose of all documents by shredding or incineration.
- At a minimum, records containing confidential data must be destroyed in this manner. Non-confidential records may be disposed of in the regular garbage removal system or by sending documents to a commercial recycling center.
- Where confidential document disposal services are contracted from an outside agency, ensure the reputation and reliability of the agency is adequately investigated.

Staffing and Monitoring Controls

The credit union should establish staffing and monitoring controls which protect against fraud, theft or misappropriation. These controls should be appropriate given the size of the organization, and the level of risk the credit union faces from such incidents. Such controls, which should be specified in policy and documented in procedures, include:

- staff supervision;
- segregation of duties;
- proper hiring practices;
- internal audit - investigation and correction of internal control weaknesses;
- board follow-up of auditor reports and on-site verification reports.

Staff Supervision

Staff supervision is a fundamental component of effective internal controls as well as part of human resource management. Two important objectives of staff supervision are:

- Quality control - which assures that adequate supervisory assistance is made available to staff in new positions, during periods of excess volume, when there is an urgent problem to resolve, and when additional expertise is required.
- Protection against fraud, theft or misappropriation - which should be pursued through the monitoring of internal controls by supervisory personnel.

Supervisory personnel must have sufficient training and experience in managing and motivating staff. Supervisors should be instructed to treat all employees equally and fairly.

Supervisory staff should be responsible for the following employee practices, and respond immediately to any irregularities that are detected:

- Require that all overtime be approved.
- Require regular vacations be taken.
- Be aware of any change in attitude or morale.
- Be aware of any change in the financial condition of an employee, which may lead to fraud.
- Require proper expense reporting (e.g. presentation of receipts).
- Conduct surprise cash counts and/or inspections of job stations.
- Encourage job rotations for new skill development.
- In situations where fraud is suspected, the internal auditor or the audit committee should review employee accounts for unusual transactions.

Segregation of Duties

Segregation of assigned staff duties is a necessary control to avoid staff error, and to avoid staff fraud or theft. The following recommendations on segregating job functions include:

- Job responsibilities of all personnel should be clearly defined before a division of duties can be properly assessed.
- An organizational chart, detailing lines of reporting, responsibility and authority.
- Written operating procedures or flow charts, is recommended in order to analyze and separate various operational processes.
- As a general rule, duties should be separated to allow for the performance of automatic checks.
- No person should be permitted to dominate a transaction from start to finish.
- Transaction initiation, authorization, custody of related assets and record keeping should be handled by independent individuals where the size and resources of the credit union allow.

Limited Resources

Where a credit union has too few employees to allow for adequate segregation of duties, certain adaptations must be made. The associated risks of unilateral control are employee dishonesty and/or a greater frequency of transactional errors, given the absence of investigative checks. The following alternative business practices are recommended to reduce these risks:

- Employees who authorize transactions may be permitted to record the transactions but should not be permitted singular custody over the related assets; e.g. these persons should neither receive nor disburse funds unilaterally.
- Cheques and large transactions should require the signature of the general manager and a board member, usually the chair.
- Members of the audit committee should review transactions processed by the general manager and staff.

Hiring Staff

The most valuable asset of the credit union is its staff. The organization, as a result, must have specific plans in place for recruiting, selecting, training and promoting its personnel. This topic is covered in other areas of this Reference Manual:

- For planning human resource requirements, refer to Section 1503 on the Human Resource Plan.
- For relevant employment legislation, refer to Section 2102 on Duty to Comply.
- For a discussion of employment discrimination and nepotism, refer to Section 2105 on Unethical Conduct.
- For a discussion of appraising staff performance, refer to Section 3101 on Staff Performance.

Each new employee should receive an orientation program to the credit union, and informational literature. The literature should include a list of job responsibilities and key performance targets, work policies and procedures, the credit union's mission statement and core values, employee benefits and the personnel policy handbook.

New staff should be required to sign a "Declaration of Ethical Conduct", in which they agree to "hold in strict confidence all transactions of members". A sample declaration is provided in the Sample Code of Conduct, which can be found in Section 2106.

The credit union should advise all staff of employee behaviour which may result in immediate dismissal (a written policy is recommended), including:

- criminal activities such as fraud, forgery, theft, larceny or any similar offence;
- violation of the Act or Regulations (including the employee's agreement to confidentiality);
- harassment of other employees;
- material insubordination;
- deliberately writing NSF cheques or cheque kiting.

Conclusion of Employment

The following activities should be carried out by management before an employee permanently departs the credit union:

- Count cash and verify other assets which may have been under the control of that employee (this should be done in the presence of the departing employee).
- Retrieve all keys, identification cards, and corporate credit cards.
- Retrieve access authorization (computer facility) and change passwords.
- Ensure no confidential information accompanies employee.

Immediately following the departure of the employee, the following activities should be carried out by management:

- Revoke the employee's signing authority (if any).
- Cancel the employee's name with the alarm company.
- Change applicable combinations and door locks.

Detecting Employee Fraud

Where an employee is suspected to be responsible for a dishonest or fraudulent act, the credit union may no longer be insured under its fidelity bond against future losses attributable to that employee.

In this case, the credit union should:

- immediately suspend the employee, with pay, until an investigation is complete;
- contact their legal counsel to determine the credit union's legal position and obligations in this situation, and whether the employee should be terminated.

Where fraud is discovered, it is recommended that the credit union:

- contact its bond insurer/master policy holder immediately after a loss is detected due to the time constraints for filing notice on bonding claims;
- inform the police, the Superintendent of Financial Services, its league, and the deposit insurer.

Role of Internal Audit

The primary objective of conducting an internal audit is to objectively evaluate the nature and quality of internal controls. Internal controls are required:

- to produce reliable accounting records;
- to determine whether board policies and board directives have been properly applied;
- to safeguard assets from fraud, theft or physical deterioration.

Internal audits should be conducted by designated internal audit staff, who are independent of the areas being audited and can report their findings to the audit committee (the audit committee will in turn report findings to the board). Alternatively, an independent contractor, the external auditor on special assignment or the members of the audit committee should execute regular inspections. (For more information relating to the roles and responsibilities of the audit committee, refer to Section 303 in the Introduction of this Reference Manual).

The recommended approach to an evaluation of internal controls is as follows:

- Conduct a system review which documents the flow of transactions in the credit union by function (e.g. loans, deposits, investments, other) through the use of narrative descriptions and/or flow charts.
- Consider the types of weaknesses that could occur from the system's current design, by individual function, and list the internal control procedures that are in place which will prevent such weaknesses.
- Compare these internal controls to what has been authorized by policy. Summarize what internal controls are missing. (The use of internal control checklists is recommended for this step. Refer to the league or an external auditor for these checklists).
- Test existing controls by reviewing historic transactions to determine compliance with expected policies and procedures. Recommend improvements to internal controls, where weaknesses are found.
- Test general compliance with by-laws, board approved policies and operational procedures.

Schedule 9.9 summarizes the recommended areas of investigation of an Internal Audit.

| Schedule 9.9 | |
|--|--|
| RECOMMENDED INTERNAL AUDIT CHECKLISTS | |
| 1. Internal Audit Planning | <ul style="list-style-type: none"> • audit emphasis and timetable • internal controls evaluation summary (sample attached) |
| 2. General Controls | <ul style="list-style-type: none"> • human resources (e.g. segregation of duties, hiring, authorization, supervision) • premises security • accounting functions and management information system |
| 3. Cash | <ul style="list-style-type: none"> • cash authorization limits and cash counts • cash records • cash shipments and storage • negotiable instruments • ATMs and night depositories |
| 4. Investments and Fixed Assets | <ul style="list-style-type: none"> • purchases • dispositions • custody controls • records and inventory counts |
| 5. Loans | <ul style="list-style-type: none"> • loan evaluations, approvals and authorizations • loan records • loan disbursements • security administration • connected party loans limits • restricted party loans limits • delinquent loans |
| 6. Shares and Deposits | <ul style="list-style-type: none"> • new and closed accounts • account records • current accounts • term and RRSP deposits • related party deposits • dormant accounts |
| 7. Revenue and Expenses | <ul style="list-style-type: none"> • revenue controls • expense controls • profitability and capital maintenance |
| 8. Computer Information System (CIS) | <ul style="list-style-type: none"> • security of the CIS • electronic and telephone banking • documentation of the CIS code • access to the CIS |
| 9. Policies and procedures | <ul style="list-style-type: none"> • test compliance with by-laws, board policies and operational procedures |

Schedule 9.10 is a sample Internal Controls Evaluation Summary which should be completed by the designated internal auditors, first on a preliminary basis, in conjunction with studying organizational and internal control designs, and then on a final basis after testing for evidence that in fact these internal controls are working.

| Schedule 9.10 | | | | |
|--|--------------------|----------|----------|-----------|
| INTERNAL CONTROLS EVALUATION SUMMARY | | | | |
| | PRELIMINARY | | | |
| | G | A | W | NE |
| GENERAL CONTROLS Conclusion | | | | |
| CASH CONTROLS Conclusion | | | | |
| INVESTMENTS & FIXED ASSETS Conclusion | | | | |
| LOANS Conclusion | | | | |
| LIABILITIES Conclusion | | | | |
| REVENUES & EXPENSES Conclusion | | | | |
| COMPUTER INFORMATION SYSTEM Conclusion | | | | |
| POLICIES & PROCEDURES Conclusion | | | | |
| Legend: G: Good A: Adequate W: Weak NE: Not Evaluated | | | | |

Where internal audit analysis is thorough and well documented, it should be shared with the external auditor who is permitted to rely on this analysis and could therefore be in a position to reduce the external audit fee.

The results of the internal audit process and follow up recommendations must be presented on a timely basis to the board and management for their review.

External Auditors

Section 159 of the Act requires a credit union, at its annual meeting to appoint its external auditors. The duty of the external auditors is to assess and report on the reliability of the organization's financial statements. Normally, the board recommends the appointment of the auditor to the general membership at the annual meeting.

Section 160 of the Act sets out qualification of auditors. The external auditors must not be anyone who is a director, officer, committee member or employee of the credit union, or who is financially associated with the same.

Audit Committee

It is part of the audit committee's function to act as liaison between the external auditors and the board. The specific duties of the audit committee in this regard are defined in section 26 of Regulation 76/95.

Scope

The external auditors begin their work by becoming familiar with the policies and internal controls of the organization, in particular its accounting procedures. Subsequently, tests of the accounting records are conducted to determine whether the records have been prepared in accordance with these policies and procedures, as well as generally accepted accounting principles, and whether these can be substantiated by evidence of the underlying transactions.

In accordance with section 167 of the Act, management must comply with the information requests and the investigative procedures of the auditors so that their work may be conducted efficiently and with sufficient scope on which to base an audit opinion.

Auditor's Report

The auditors' report, when completed, should be shared with management and the audit committee. It is the audit committee's function to report the findings to the board of directors for follow-up. Finally, the auditors are required to present their report to the membership at the annual meeting in accordance with section 169(2) of the Act.

Section 172 and the Management Letter

Section 172 requires auditors to report to the general manager, the audit committee and the board of directors, any transaction or conditions that have come to the auditor's attention affecting the well being of the credit union, that, in the auditor's opinion, are not satisfactory and require rectification.

Such transactions or conditions can include, but are not limited to:

- transactions not within the powers of the credit union, as defined in the Act or the credit union's by-laws;
- large loans (defined as greater than one half-per cent of total assets) where, in the opinion of the auditor, loss is likely to occur;
- any circumstances which indicate there may have been a contravention in the Act or Regulations.

The form of the section 172 report should be a letter to the board, general manager, chief financial officer and audit committee, acknowledging that section 172 of the Act had been considered in the course of the annual audit, and indicating whether there are any reportable transactions pursuant to that section. This letter is commonly known as a management letter or derivative report.

Any reportable transactions or conditions should be specified in the letter, together with recommendations for rectifying or addressing the transaction/condition. The management letter should be reviewed by the audit committee and the board of directors. Recommendations in the letter must be discussed, addressed and resolved to the satisfaction of all parties. If there are no reportable transactions or conditions, then the management letter should still be prepared, with comments to this effect.

Finally, a copy of this report should also be provided to the Superintendent of Financial Services, DICO and the stabilization authority for that credit union.

Audit Committee and Board Follow-up

To complete the function of monitoring internal controls, the audit committee and the board must review the information that it receives regarding internal controls. This information comes from a variety of sources, including:

- the report of the internal control audit;
- the external auditor's report including the section 172 management letter;
- on-site verification reports by DICO.

The board and the audit committee must ensure that recommendations in these reports are be discussed, addressed and resolved to the satisfaction of all parties. Management should be required to report back to the board when adopted recommendations are complete.

Policy Development and Review

The board is required to develop policy to manage risk within the credit union. It is also required to annually review board policies, to ensure that they are current and appropriate. The review of policy can be delegated to a sub-committee of the board. The approval of new or amended policies, however, can not be delegated, and is a function of the board.

Some credit unions may request management to draft their policies; however, the Board's analysis and final approval should always be obtained. Policies are required to be in writing so that they are not vulnerable to misinterpretation particularly as a result of staff turnover.

It is recommended that policy statements be placed in a Board Policy Manual. A Policy Log should be kept as part of the Manual, which lists all board policies, and the dates they were implemented. The Log should also be used to keep track of and administrate the review of board policies. A sample Board Policy Log is provided in Schedule 9.11.

To ensure that policies have sufficient scope and content, the board should consult appropriate sections of the Act and Regulations (specifically, sections 104, 190 and 191 of the Act, sections 50, 78 and 87 of Regulation 76/95, and FSCO's Guideline for Prudent Investment and Lending Policies and Procedures for Ontario's Credit Unions).

| Schedule 9.11 | | | | |
|--|--------------------|---------------------|---------------------|---------------------------|
| SAMPLE BOARD POLICY LOG | | | | |
| Policy area | Created on: | Last review: | Next review: | To be reviewed by: |
| <ul style="list-style-type: none"> • Governance • Capital Management • Credit Risk Management • Market Risk Management (Investments) • Structural Risk Management (Asset/Liability) • Liquidity Risk Management • Operational Risk Management (Internal Controls) | | | | |

Technology Development

The level of technology employed should support future business and strategic plans of the organization.

New or modified systems hardware or software must be appropriately authorized and fully tested prior to going on line and should not be implemented without proper documentation and adequate training.

Institutions should establish an appropriate framework for technology development.

This framework should include processes for:

- planning for technology requirements consistent with business strategies and activity needs
- 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.

Outsourcing of Services

Outsourcing involves 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

Overview

Appropriate rationale and business case should be developed to support recommendations for outsourcing services. Services or functions that are typically considered for outsourcing include:

- investment management
- information systems management
- lending analysis and/or loan collection activities
- records management
- payroll administration
- internal audit.

Sufficient analysis should be undertaken to confirm that the service provider has the necessary expertise, capacity and viability to perform the functions or activities to be outsourced. Appropriate due diligence and impact analysis of non-performance by a service provider should also be undertaken.

All outsourced services should 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.

A review of the service provider's performance should occur at a minimum annually, and align with the length of the contract. 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.