

**NOVA SCOTIA CREDIT UNION
DEPOSIT INSURANCE
CORPORATION**



**INTERNAL CONTROL PRACTICES
AND PROCEDURES**

BEST PRACTICES DOCUMENT

Revised February 2009



INTERNAL CONTROL PRACTICES AND PROCEDURES BEST PRACTICES DOCUMENT

TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	INTERNAL CONTROL PRACTICES AND PROCEDURES.....	3
2.1	CONTROL OF INTERNAL ACCOUNTS.....	3
2.2	AUDIT OF REPORTS.....	5
2.3	OPENING AND CLOSING PROCEDURES.....	6
2.4	PREMISE SECURITY.....	7
2.5	OFFICE KEYS AND LOCKS.....	8
2.6	OFFICIAL SIGNING AUTHORITIES.....	8
2.7	CASH HOLDINGS AND SECURITY.....	9
2.8	SURPRISE COUNTS.....	10
2.9	CASH OVER AND SHORT.....	10
2.10	CHEQUE CASHING.....	11
2.11	ATM / CDU.....	11
2.12	NIGHT DEPOSITORY	12
2.13	RECORDING IN-TRANSIT DEPOSITS.....	12
2.14	INCOMING, OUTGOING AND RETURNED MAIL.....	13
2.15	COMBINATIONS & ALARM CODES.....	13
2.16	SUPERVISORY LEVELS AND CHANGING OF PASSWORDS.....	14
2.17	SAFEKEEPING OF SECURITIES.....	14
2.18	SAFETY DEPOSIT BOXES.....	15
2.19	SAFEKEEPING OF RECORDS.....	15
2.20	OFFICIAL CHEQUES	16
2.21	TRAVELER'S CHEQUES	16
2.22	MONEY ORDERS.....	17
2.23	CHEQUE WRITER / PERFORATING EQUIPMENT	19
2.24	COMPUTER FILE BACKUPS.....	19
2.25	NEW CUSTOMER-OWNER APPLICATION AND IDENTIFICATION.....	20
2.26	CLEARING.....	20
2.27	INACTIVE AND DORMANT ACCOUNTS, AND UNCLAIMED BALANCES	21
2.28	STAFF MEMBER ACCOUNTS, LOAN & CREDIT FILES AND PRIVACY CONSENTS.....	22
2.29	PROFESSIONAL CONDUCT, CONFIDENTIALITY AGREEMENT & CONFLICT OF INTEREST DISCLOSURE.....	22
2.30	MANAGEMENT, STAFF, BOARD AND COMMITTEE EXPENSES.....	23
2.31	CREDIT UNION OPERATING EXPENSES.....	24
2.32	REPORTING TO THE BOARD OF DIRECTORS.....	24
2.33	MEETING AGENDAS	25
2.34	RECORDING OF MEETING MINUTES.....	26
2.35	MONEY LAUNDERING REGIME AND COMPLIANCE.....	27
2.36	DELEGATION OF LENDING LIMITS & DISBURSAL OF LOANS.....	27
2.37	PROTECTION OF PERSONAL INFORMATION.....	28
2.38	POS, ATM AND ICU LIMITS, MEMBERCARDS AND CONTROLS.....	29

**INTERNAL CONTROL PRACTICES AND PROCEDURES
BEST PRACTICES DOCUMENT
As Issued by the Nova Scotia Credit Union Deposit Insurance Corporation**

1. INTRODUCTION

For an internal control system to be adequate, appropriate segregation of duties, accountability and audit trail must be evident within each element of the credit union operation. The main focus is to minimize the opportunity for employees to be given undue ability to engage in improper behaviour which could seriously impact staff morale and image of the credit union and network. The following is by no means meant to identify all internal control systems. These responsibilities reside with management and the board. The objective is to identify the areas in the credit union operation, which are most susceptible to risk and to ensure there are sufficient and effective preventive and detective control mechanisms in place. Please note that a significant portion of the information provided below was taken from the SECURITY PROGRAM MANUAL available on the Credit Union Central of Nova Scotia (CUCNS) website where ongoing updates are being made to the document.

The development of the Internal Controls Review Program is ongoing and periodic updates will be made to this document.

For more information, please contact Norbert E. Gagnon, Analyst, at the Nova Scotia Credit Union Deposit Insurance Corporation (CUDIC) by using the toll-free number 1.877.770.5622, direct phone: 902.490.2156 or email: gagnonne@nscudic.org.

2. INTERNAL CONTROL PRACTICES AND PROCEDURES

2.1 CONTROL OF INTERNAL ACCOUNTS

Internal Control Objective:

To ensure appropriate controls in the administration of internal accounts are in place and to confirm all internal accounts are being properly reconciled and cleared on a timely basis.

Best Practice:

- Responsibility for daily verification of reports clearly documented and understood by staff.
- Segregation of duties, accountability and audit trail evident in the practices and procedures used for the control of all internal accounts.

Note - It is a **good practice** to rotate amongst staff the responsibilities for completing and checking the reconciliation of internal accounts. This strengthens the internal controls and promotes cross training.

- Internal accounts no longer in use are closed.
- Signature cards available for all internal accounts.
- Formal month-end reconciliation completed for each internal account with a closing balance other than zero showing on the month-end statement. The back of the original month-end statement used to complete the reconciliation, all outstanding deposits and withdrawals (debits and credits) listed, and the net effect is zero.

Note - If an original month-end statement is not automatically produced, one must be printed from the data system. Use of a PC Excel spreadsheet for the reconciliation of internal accounts is acceptable if the structure of the information is the same as the back of the original statement. Excel spreadsheet password protected with access restricted. Other procedures may be acceptable as long as the same objectives are achieved.

- Sufficient information included on the reconciliation with each outstanding item to provide a proper audit trail for future follow up / verification (e.g. for outstanding deposits – date of deposit or credit memo, origin/description and amount; for outstanding withdrawals – cheque identification number, date cheque issued or debit processed, amount and payee / origin / description.)

Note - If the outstanding items are too numerous to list on the back of the original statement for reconciliation, it is acceptable to run a tape of the cheques and enter the cheque number (and date issued if space permits) beside the amount on the tape. Then attach the tape to the original statement where the reconciliation is done. The corresponding total from the tape would be entered in the appropriate area on the back of the original statement for reconciliation purposes.

- An addition tape of the outstanding items proving the reconciliation to zero attached to the statement. The clear symbol evident on the adding machine tapes.
- Reconciliation dated and initialled / signed on the back of the original statement and on the adding machine tape by the person who completed it. Another person, preferably a supervisor, checks and initials the reconciliation and tape to confirm the reconciliation was properly completed.

Note - When the closing balance showing on an internal account month-end statement is zero, it is acceptable for the person responsible for completing the reconciliation and the person checking it to simply initial beside the zero balance on the statement.

- Follow up conducted for all items that are outstanding over six months. Follow up activity documented.
- Practices and procedures consistent in all branches.

The following lists examples of internal accounts that could exist in credit union branches either under an account or general ledger number that may be reviewed by CUDIC during an Internal Controls Review. Other accounts may also be reviewed:

Canada Custom and Revenue Agency	Internal Current Account (Official CU Chequing)
Canada Savings Bonds Holding	IWK Fundraising
Canadian Money Orders	M/C Debit Card Staff Expense
CDI Commission	Municipal Taxes
CDI/CLI Accounts Payable	Non-Posted Clearing Items
CDI/CLI Premiums & Refunds	Non-resident Withholding Tax
Certified Cheques	Payroll
CLI Commission	PPSA – Security Agreement Registration
Credential Asset Management Inc. “In Trust”	RRSP/RRIF Withholding Tax

CU Charitable Foundation	School Credit Union Account
CUC Current Account	Staff Fund Account
CUETS Billing – Revenue & Expenses	Suspense Accounts
CUMIS EFT Holding – Disability Claims Payments	Teller Cash Transfer/Contra Account
CUMIS Insurance – Disability Claims Payments	TelPay (Main Sweep) Account
Ethical Funds – Trailer Fees	TelPay (OTC) Over-The-Counter
Fundraiser/Donation Account	TelPay/MemberDirect (via Phone & Website)
Hold Funds Account	Travel Insurance
Holding Account for Returned Cheques	Traveler’s Cheques
Inactive/Dormant Accounts	US Money Orders
Inter-Credit Union (ICU) Banking (Acculink/Masterlink) – Turbo	Utility Account or Utility Remittance Holding

2.2 AUDIT OF REPORTS

Internal Control Objective:

To ensure critical data reports are reviewed under appropriate segregation of duties on a timely basis and to ensure timely management response and follow-up of exceptional items in order to limit the credit union’s exposure to unauthorized or erroneous transactions.

Best Practice:

- Consistent acceptable practices and procedures exist in all branches.
- The validity of each change/transaction verified to a properly completed and authorized source document that supports the change or advance.
- Segregation of duties and cross checking to provide accountability exists throughout the credit union. Management and staff responsible for checking, monitoring and authorizing indicate they have done so by initialling the reports or the specific changes or items on the reports for accountability.
- Records retention meets Canada Customs and Revenue Agency, External Auditor, CUDIC and legislative requirements.

CGI/League Data Reports reviewed during an Internal Controls Review by CUDIC normally include but not limited to the following:

Rpt #	Report Name	Frequency
005-1	Changes to Member Records	D
005-2	Changes to ELS Records	D
010-1	Changes to Deposit Account Records	D
014-1	PCA Line of Credit	D
014-2	PCA Overdrafts	D
014-3	Overdrawn Shares and Savings	D
028-2	Term/RRSP/RRIF Maturity Errors	M

Rpt #	Report Name	Frequency
029-3	Non-posted Direct Deposits	D
036-1	Prepaid Loans	M
046-1	Daily List of Loan Advances	D
047-1	List of Loans Paid Off	W
054-1	Changes to Loan Records	D
058-1	New and Closed Customer-owners	M
089-1	Loan Maintenance Errors (Monthly)	M
097-1	Trial Balance by Interest	D
097-2	Trial Balance by Sub-Class	D
120-1	General Ledger Year to Date (Daily - used with teller blotter)	D
163-1	General Ledger Year to Date (Monthly)	M
186-1	New Member Records	D
186-2	New ELS Records	D
187-1	New Deposit Account Records	D
188-1	New Loan Records	D
198-2	RRSP Errors	M
203-1	Changes to Service Records	D
250-2	Card Orders Errors	D
285-1	Teller GL / Cash Errors	D
292-1	Posted Issuer ATM Transaction	D
292-2	Posted Issuer Direct Payment Transaction	D
319-2	Transaction Messages	D
319-4	Non-Posted GL Integration Errors	D
320-1	Non-Posted Account Transactions	D
335-1	Membership Activity Monitoring	M
337-1	Changes to Service Charge Records	D
337-2	New Service Charge Records	D
375-1	Interest Rate Changes	OL
380-1	Non-Posted G/L Errors	D
447-1	New/Changes AFT Records	D
481-1	Changes to Multi-Level Records	D
533-3	Non-Posted Direct Deposits and Pre-Authorized	D
547-1	RRIF Payment Errors	D
558-1	New/Changes to Auto Transfers	D
565-1	Suspicious Activity	D
635-1	GL Auto Balance	D
643-1	CAD Money Transfer Listing	D
644-1	USD Money Transfer Listing	D
666-1	Changes to Integration Records	D

Note:

A full list of reports providing information regarding frequency, recommended actions, retention periods, supervisory/management review can be found on the Credit Union Central of Nova Scotia's website under Reference\NS&NL Manuals\Banking System Reports.

2.3 OPENING AND CLOSING PROCEDURES

Internal Control Objective:

To ensure proper premises opening procedures are in place so credit union employees do not find themselves in a hostage situation and to ensure proper premises closing procedures are in place to appropriately protect staff and credit union assets.

Best Practice - Openings:

- All clear signal or system including a status check code word used.
- All clear signal changed quarterly or more often if required.
- Survey of surrounding area conducted before approaching premises.
- Only one staff enters and checks premises to ensure all is in order.
- All other employees remain outside building until all clear signal evident.
- Staff informed of required process, including status check code word, if all clear signal not executed within defined time.
- Staff informed on procedure to follow if no clear signal given or there's evidence of a break in.
- Opening procedures are documented.
- Opening procedures reviewed with all new staff and at least annually with all staff.

Best Practice - Closings:

Where staff complements permit, two designated staff members are present for lock-up. Prior to leaving, they ensure:

- All doors and windows locked and checked thoroughly for damage and improper locking mechanism.
- All rooms, closets and basement checked to ensure all persons, especially someone unauthorized to be there, have left building.
- Cash drawers and anti-holdup units empty and left open with keys removed.
- All securities and records put away in their appropriate cabinets and locked.
- Certified cheques and other stamps locked away.
- Cheque writer and postage meter locked; the keys removed and placed in vault or appropriate location. Note - If possible, the cheque writer should be placed in the vault.
- All money orders, traveler's cheques and official cheques locked in the vault/safe compartment. Control logs placed in appropriate location separate from pertinent negotiable instruments.
- Wastebaskets not to contain confidential information.
- Computer terminals exited and logged off.
- Proper alarm procedures followed to prevent false alarms.
- Where applicable, microfilm camera unit medium stored in a fireproof location.
- Main vault/safe locked unless two employees are present.
- Time lock for safe or vault set for the next business day.
- All vaults, safes and filing cabinets locked and keys removed.
- Nightlights left on particularly over the vault or safe and record cabinets. Outside lights also remain on, especially over parking lots and front and rear exits.
- Window drapes open to provide full view of premise interior at night.
- Exterior area of door being used by employees for exiting the building surveyed before the premise alarm is set and door locked.
- Closing procedures are documented.

Consideration should be given to having a Crime Prevention Through Environmental Design (CPTED) site review completed by the local RCMP. For further information, contact the Risk Management Services at CUCNS.

2.4 PREMISE SECURITY

Internal Control Objective:

To ensure the exits from and to the credit union premises and the security systems provide appropriate protection for staff, customer-owners and credit union assets.

Best Practice:

- All staff and visitors permitted to enter the credit union only through the main entrance(s). Other entrances used for emergencies only.
- During non-business hours, all entrances remain locked.
- All exit doors have a window or peephole providing a reasonable view of the immediate area should they have to be opened for any reason. Use of exits other than the main entrance to the credit union premises by staff or anyone else strongly discouraged. As much as possible, rear or side exits used as fire exits only. If staff members use rear or side exits for breaks or other reasons, area surveyed before exiting to ensure it is safe to do so, the door locked behind them and only opened by someone from the inside. Otherwise, only the main entrance used.
- Security camera systems checked daily to ensure properly functioning, direction of camera(s) provide ultimate / best image surveillance and usefulness of recording tested weekly.

2.5 OFFICE KEYS AND LOCKS**Internal Control Objective:**

To ensure appropriate control is maintained over credit union premises keys.

Best Practice:

- All outside premise doors installed with good quality locks for which keys are registered and cannot be duplicated without proper authorization.
- A custodian of keys designated and a key register maintained for all keys.
- Keys restricted to only employees responsible for opening/closing procedures.
- Recipients sign for keys issued.
- All persons assigned a key return the key upon leaving employment/service. All returned keys recorded in the key register.
- Building key locks changed/re-keyed each time an employee who holds keys leaves the employ of the credit union if the key can be readily duplicated.
- All duplicate/spare keys are stored in a locked compartment in the safe/vault, preferably under dual control.

2.6 OFFICIAL SIGNING AUTHORITIES**Internal Control Objective:**

To ensure the credit union has established appropriate signing authorities.

Best Practice:

- Resolution from the Board of Directors approving a policy and designating signing authorities on behalf of the credit union with and without the corporate seal and for all internal accounts (normally under Policy Section 11000, Subsection 11250).
- If signature limits delegated, receipt of policy and delegated signing authority formally acknowledged by signer.
- Signature card completed for internal accounts in each branch.
- Signing authorities registered with CUCNS Treasury & Payment Services for all accounts held at CUCNS are the same as those recorded in the credit union records.

2.7 CASH HOLDINGS AND SECURITY**Internal Control Objective:**

To ensure the credit union cash holdings are appropriately secured.

Best Practice:

- If the credit union offers foreign currency accounts, a foreign exchange policy approved by the Board of Directors that establishes an acceptable exposure limit, time expectations for correcting exposures; and the type of transactions and currencies supported, authorization limits and reporting expectations.
- Documented procedures covering the monitoring and balancing of foreign currency assets and liabilities, the reconciliation of internal foreign currency bank accounts, the frequency and requirements of reports to management, the review of general ledger accounts used for foreign exchange transactions, and quarterly compliance reporting for the board.
- Each teller/supervisor involved in cash holdings and security to receive a formal designation of cash holdings, cheque cashing and cash withdrawal limits and formally acknowledge same.
- Ongoing supervisory monitoring of teller cash holdings for adherence to designated limits.
- Cash holdings for the credit union monitored to determine if the insurable limits are being respected and to identify potential risks or concerns. Exceptions communicated to management.
- Security and best practices include:
 - Vault/safe door opened under dual control, bolt turned in closed position and one combination spun once opened.
 - Teller stamp secured and cash drawer locked with key removed when teller leaves station.
 - If installed, anti-holdup units used for intended purpose.
 - Teller cash drawer, teller stamp and locker under single control (i.e., not shared).
 - Teller cash drawer and anti-holdup unit left open and keys removed when not in use.
 - Treasury accessed under dual control and access during business hours minimized.
 - Delayed action timelocks (DAT) used as required.

- Incoming and outgoing cash parcels logged, prepared and received under dual control. Preparation and verification normally done during non-business hours. Cooling off period implemented for incoming parcels.
- Transfer of cash between tellers/treasury properly controlled and documented (i.e. register, contra slips and GL entries).
- Bait money changed at least semi-annually, properly recorded (i.e., each bill number) and record held in safekeeping under dual control. Bait money in Treasury consists of an entire bundle of bills. A minimum of \$250 used as bait money in each teller's cash. If dye packs used, function tests are conducted as recommended.
- If applicable, dye pack transmitter system (or CPS system if applicable) tested annually by system installer to confirm properly functioning.
- Teller Profile on banking system matches the assigned cheque cashing and cash limits.

2.8 SURPRISE COUNTS

Internal Control Objective:

To ensure the credit union has established periodic independent surprise counts to identify discrepancies and reduce the risk of losses of cash, negotiable instruments, and cards.

Best Practice:

- Quarterly random surprise count for teller cash, treasury, ATM/CDU, money orders (Canadian and USD), traveler's cheques, InstantCards, and internal corporate cheque supply.
- Surprise cash counts conducted by supervisor, logged on the teller's blotter and register and formally acknowledged by teller and supervisor as being accurate.
- Surprise counts for other items counted and verified by a non-custodian but in the presence of the custodian. All verifications documented, dated and signed by both.

2.9 CASH OVER AND SHORT

Internal Control Objective:

To ensure discrepancies in tellers cash are appropriately investigated and addressed.

Best Practice:

- Daily verification by supervisor that tellers are in balance.
- Immaterial dollar limit where cash may be considered balanced without further investigation / search established based on credit union tolerance policy.
- Cash differences are investigated and corrected or if not located written off and properly recorded in General Ledger with corresponding notations made on teller blotter.
- All write-offs authorized by Management or designate in accordance with policy.
- Cash short and over accounts on the general ledger reviewed monthly to confirm all discrepancies appropriately approved.

2.10 CHEQUE CASHING

Internal Control Objective:

To ensure appropriate controls exist for the cashing of cheques for customer-owners, non-customer- owners, new accounts, foreign and domestic currency cheques.

Best Practice:

- Cheque cashing policy in place for domestic and foreign currency transactions processed for new accounts, existing customer-owners and non customer-owners.

Note - Recommended hold on funds (e.g. CAD – 10 days, USD – minimum 30 days).

- Staff written acknowledgement of cheque cashing policy and the individual cash limits assigned to them reviewed annually.

2.11 ATM/CDU

Internal Control Objective:

To ensure appropriate controls over the Credit Union Automated Teller Machines and Cash Dispensing units.

Best Practice:

- Documented procedures / policy in place for ATM / CDU operations.
- Cash holding limit established. Acknowledged in writing by the custodian(s) of the ATM.
- ATM room kept locked. ATM/CDU alarmed.
- Dual combinations under dual control for access.
- ATM/CDU serviced and balanced under dual control during non-business hours.
- ATM/CDU access card and room key kept in secure place and restricted to those responsible for access and balancing. Sharing of access card PIN restricted.
- Daily servicing/balancing reports and verification of deposits signed / initialled by two staff attending.

Note: Dual control over the envelopes and contents must be maintained from the time the envelopes are removed from the ATM until the envelope contents have been verified, and the appropriate postings have been made and the cash/cheques secured.

- ATM Information Report 531-1 used to balance cash.
- Holds placed on deposits until verified. Consideration given to different time zones before releasing hold when deposit made abroad.

Note: Daily CGI/League Data report 665-1 reports all deposits performed by the credit unions customer-owners since 5pm the previous day.

- Physical cash count conducted under dual control at least weekly and count documented.

- After hours servicing of ATM by credit union staff meet practices recommended under Risk Management Bulletin RM 07-05.

2.12 NIGHT DEPOSITORY

Internal Control Objective:

To ensure appropriate control of the night depository and its contents are in place.

Best Practice:

- Documented procedures in place for the control of night depository.
- All customer-owners receiving keys sign a Night Depository Agreement.
- A record maintained of all keys assigned to customer-owners.
- Extra keys for the night depository held in safekeeping under dual control.
- Night Depository opened under dual control and prior to business hours.
- Contents of the depository verified under dual control and recorded immediately in the Night Depository Register, the number of bags and envelopes and specifics of each recorded.
- Errors reported to supervisor and noted in register. Customer-owner contacted and advised on the same business day the error is identified.
- Each staff member involved in verification of deposits (including receiving teller) initials the Night Depository Register to confirm contents of deposits.
- Changes made to Night Depository Register initialled by all involved.

2.13 RECORDING IN-TRANSIT DEPOSITS

Internal Control Objective:

To meet the requirements for insurance coverage under the Master Bond for deposits lost in transit.

Best Practice:

- Both sides of each item in the deposit microfilmed, photocopied, or otherwise electronically recorded, or specified particulars recorded in writing or on a tape recorder.
- Imaging equipment regularly verified to ensure functioning properly and images readable / printable.
- Regular backup and testing of electronically stored information.

2.14 INCOMING, OUTGOING AND RETURNED MAIL

Internal Control Objective:

To ensure appropriate controls over incoming, outgoing, and returned mail.

Best Practice:

- Access to mailbox key(s) restricted.
- Mail picked up by two staff members and remains in dual custody until opened and recorded.
- Mail opened under dual control and deposit transactions recorded in a mail register. Both staff initial mail register and transaction slips confirming the amount verified.

- Outgoing mail contains the return address of the credit union's head office.

- Returned mail opened, recorded in a designated log and secured under dual control. Both staff to initial the log.

- Returned mail investigated (i.e. address verified, reason for being returned, etc.) and results along with action taken documented in log.

2.15 COMBINATIONS & ALARM CODES

Internal Control Objective:

To ensure appropriate controls over the credit union's combinations and alarm codes.

Best Practice:

- Combinations changed at least every six months and when a staff member leaves or is assigned new duties.

- Each combination stored in a sealed envelope, dated and signed across the seal by the employee responsible.

- Combination envelopes assigned to a senior staff member who is responsible to ensure their safekeeping preferably off-premises in a secure location under dual control (e.g. at another branch if a multi-branch operation).

- Presence of senior officer together with another employee required to open combination envelope.

- Combinations serviced at least annually.

- Combination register maintained. Register indicates assignments, all changes including the dates, and dates of servicing for each combination.

- All staff instructed on how to open main vault door from inside if locked in.

- Alarm codes changed once a year or upon affected staff change (recommended practice).

- Credit union has documented procedures on how to handle after hours alarm calls including completion of alarm response form available in CUCNS Security Program Manual (on CUCNS website).

2.16 SUPERVISORY LEVELS AND CHANGING OF PASSWORDS

Internal Control Objective:

To ensure appropriate restrictions are in place to provide the necessary controls over the ability to perform transactions to customer-owner accounts, credit union accounts and other records. Also, to ensure assigned supervisory levels reflect appropriate authority levels.

Best Practice:

- A full review by management at minimum every six months of all user profiles to ensure only authorized staff has the ability to process cash transactions, perform supervisory overrides, establish and/or change customer-owner records, and/or change critical credit union operating parameters such as interest rates, service development records, and service charges.
- The assignment of Administrative Teller (998) profiles that allow the user to make changes to other user profiles is restricted to senior management.
- Weekly audit by management of additions, deletions, or changes to user profiles.
- Staff/teller passwords changed at least every six months to minimize the opportunity for misuse of authority and for the protection of staff.
- Sharing of teller numbers and passwords not permitted.
- Teller numbers and ID's specific to one person (i.e. no duplicate letters to be used for teller "short name").
- No use of non-integrated tellers.

2.17 SAFEKEEPING OF SECURITIES

Internal Control Objective:

To ensure appropriate controls exist for safekeeping of securities and documents.

Best Practice:

- Securities and documents belonging to the credit union and the security provided to the credit union by customer-owners as collateral to loans kept in a locked compartment of the vault/safe under dual control.
- Safekeeping services for customer-owner securities or other valuables discouraged. Customer-owners encouraged to use safety deposit boxes.
- An accurate and detailed record maintained for all securities taken into credit union custody and the reason the security was taken. A security control log maintained for recording the description of securities and other items e.g. keys, etc., being placed in safekeeping, date received, returned, etc. together with the initials/signatures of the two credit union staff accessing safekeeping.

- Acknowledgement and receipt for securities provided to the customer-owner by two staff members. Upon return of the security, customer-owner required to sign for receipt of the item. Records maintained.
- Physical verification of the contents of the compartment to the log completed at least every quarter under dual control and a record in support of this being done maintained.

2.18 SAFETY DEPOSIT BOXES

Internal Control Objective:

To ensure appropriate controls exist for the operation of credit union's Safety Deposit Box service.

Best Practice:

- Documented procedure covering all areas of operation for safety deposit boxes.
Note: Refer to CUCNS issued Procedures Manual section 4.1 (Jan/08). If this procedure is not adopted, the credit union should formulate one with similar content.
- Customer-owners sign a fully completed Safe Deposit Box Agreement (including all Terms and Conditions) and Rental Record. Signatures are witnessed.
Note: Refer to CUCNS developed form CUC361 Rev 01/08.
- A Safety Deposit Box Access and Index card used to record any access provided to the safety deposit box. Customer-owner and staff providing access each sign card.
Note: Refer to CUCNS developed form CUC363.
- Agreements and access cards stored in vault.
- Customer-owner completes the "SURRENDER" Agreement and returns both keys upon cancellation of safety deposit box service.
- Keys to non-rented boxes kept in safekeeping, under dual control, where possible.
- Prep keys accessible to authorized staff only. Spare prep keys held in safekeeping under dual control.

2.19 SAFEKEEPING OF RECORDS

Internal Control Objective:

To protect the confidentiality of customer-owners' personal information and to ensure security safeguards are appropriate to the sensitivity of the information.

Best Practice:

- Authorized staff working with customer-owner information (files, reports, documents, etc.) demonstrate care to ensure the protection and confidentiality of that information. Information always put away/secured before inviting another customer-owner into the office.

- Current files/documents (e.g., membership applications, loan applications, credit reports, security documents, etc.) of customer-owners appropriately secured in locked filing cabinets and access restricted to authorized personnel.
- Miscellaneous paper containing any customer-owner or account information properly disposed of by immediate shredding or by placing in shredder box for secure disposal.
- Retention of other records and reports to comply with CUDIC, audit and legislative requirements. Documents appropriately secured and access restricted to authorized personnel only.

2.20 OFFICIAL CHEQUES

Internal Control Objective:

To ensure the safeguard and control of unissued cheques and issued official cheques are properly authorized and signed by the required authority level(s).

Best Practice:

- Main supply of credit union official cheques stored in a locked vault/safe compartment under dual control, sole custody.
- Working supply kept in a secure place during business hours and controlled by a designated custodian who ensures supply is locked in the vault/safe at night.
- Official cheques checked monthly to ensure that numbers are sequential and all numbers have been accounted for.
- Two authorized signatures required on all official cheques; official cheques never pre-signed. Amounts perforated using cheque writer/perforating equipment.
- Issued official cheques do not exceed authorized limits.
- Spoiled cheques cancelled by cutting out the signature area and writing "void" across the face of the cheque. Spoiled cheques attached to cheque register and/or stub.
- All issued and spoiled cheques recorded in the official cheque register and/or stub.
- Monthly reconciliation of official cheque account completed by an employee who is not responsible for issuing cheques. Completed reconciliation checked by another staff member. Monthly review by management.

2.21 TRAVELER'S CHEQUES

Internal Control Objective:

To ensure the custody and issuance of travellers cheques is appropriately managed and controlled.

Best Practice:

- Traveler's cheque register kept to properly record all cheques sold and on hand. Cheques recorded by serial number and denomination and by date received or sold.
- Register kept in a secure location separate from the supply of traveler's cheques. Transactions recorded in Register and initialled by two staff members.
- Incoming traveller's cheques counted and verified under dual control.
- Main supply of traveler's cheques stored in a locked vault/safe compartment under dual control, sole custody.
- Working/day supply verified daily and kept in a secure place during business hours under the control of a designated staff member or is disbursed to individual tellers to include in their cash holdings. Supply locked in the vault/safe at night.
- At least quarterly, surprise count of traveler's cheques completed and reconciled to register. Count performed by an employee who is not responsible for handling the cheques.
- Settlement made in accordance with the traveler's cheque company requirements.
- Traveller's cheques on hand do not exceed limits set by the issuing company.

2.22 MONEY ORDERS

Internal Control Objective:

To ensure the custody and issuance of money orders is appropriately managed and controlled.

Best Practice for Money Orders issued in Canadian Funds:

- Money orders register kept to properly record all money orders sold and on hand. Register stored in a secure location separate from the supplies.
- Incoming money orders counted and verified under dual control. Money orders recorded by serial number in the register the same day as received. Initials of the two individuals who verified the incoming supplies recorded in the register.
- All sales of money orders recorded in the register on the date of sale and initialled by staff selling instrument. The name of the person and/or customer-owner account number and contact number to whom the money order was sold recorded in the register or on the credit union's copy of the duplicate for future reference and follow up.
- Amounts perforated using cheque writer/perforating equipment.
- Main supply of money orders kept in a locked compartment in the vault/safe under dual control, sole custody.
- Working/day supply verified daily and kept in a secure place during business hours under the control of a designated staff member or disbursed to individual tellers to include in their cash holdings.
- Working supply replenished before opening for business or after close and supply locked in the vault/safe at night.

- Spoiled money orders properly cancelled by cutting out the sender's signature area writing "void" across the face of the money order. Recorded as "Void" in the money order register and the voided item attached.
- Money orders outstanding for more than six months followed up in an attempt to clear the item(s). Items, which cannot be traced due to lack of information or inability to locate the purchaser, transferred to an inactive/dormant account or revenue/income GL account once the item has been outstanding for over a year. All follow-up activity documented.
- An appropriate monthly reconciliation of the internal account for Money Orders completed by a staff member not involved in the sale of money orders. Reconciliation checked by another staff.
- Surprise counts of unsold money orders and reconciliation to the Money Order Register performed at least quarterly by an employee not responsible for the handling of money orders.

Best Practice for Money Orders issued in US Funds:

- Money orders register kept to properly record all USD money orders sold and on hand. Register maintained in a secure location separate from the supplies.
- Incoming USD money orders counted and verified under dual control. USD money orders recorded by serial number in the register the same day. Initials of the two individuals who verified the incoming supplies recorded in the register.
- All sales of USD money orders recorded in the register on the date of sale and initialled by staff selling instrument. Issued USD money orders do not exceed the maximum value outlined in the Money Order Agreement. Settlement made in accordance with the Credit Union Central requirements.
- The sale of a USD money order and completion of the draft made in accordance with procedures issued by Credit Union Central (Treasury and Payments).
- Main supply of USD money orders kept in a locked compartment in the vault/safe under dual control, sole custody.
- Working/day supply verified daily and kept in a secure place during business hours under the control of a designated staff member or is disbursed to individual tellers to include in their cash holdings.
- Working supply replenished before opening for business or after close and locked in the vault/safe at night.
- Spoiled USD money orders properly cancelled by cutting out the sender's signature area writing "void" across the money order. Recorded as "Void" and \$0.00 in the USD money order register and the voided item attached.
- A surprise count of unsold U.S. money orders and reconciliation to the USD money order register performed at least quarterly by an employee not responsible for the handling of USD. money orders.

2.23 CHEQUE WRITER / PERFORATING EQUIPMENT

Internal Control Objective:

To safeguard against unauthorized use of cheque writer equipment.

Best Practice:

- Equipment is locked and the key is placed in the vault/safe at night.

Note - Although it would be preferred that the entire unit be stored in the vault/safe at night, it is understood this will not always be possible because of the weight of the unit and space available in a safe.

2.24 COMPUTER FILE BACKUPS

Internal Control Objective:

To ensure the credit union has implemented appropriate computer system security and protection of information.

Best Practice:

- Only licensed software maintained on credit union personal computers (PC) and servers. Listing of authorized software maintained.
- Credit union staff or outsource partners have the appropriate media to restore or install appropriate hardware.
- Credit union network, PC and servers appropriately protected from unauthorized access by appropriate firewall hardware and software rules, and appropriate anti-virus software in place to limit exposure to computer virus intrusion.
- Appropriate uninterruptible power supply devices (UPS) implemented to protect critical IT equipment in the event of power interruptions and power surges.
- Periodic review of employee PC's and credit union servers to ensure installed PC and Server software is limited to approved software types and versions, and to ensure periodic updates and upgrades are completed so that only current supportable software versions are in use.
- Staff advised in writing to save all critical documents and e-mail to a shared server that is being backed-up on a nightly basis.
- Backups stored off-site in a secure, environmentally appropriate storage area (e.g. protected from water, fire, heat, damage).
- Periodic review by supervisor that confirms backup.
- Business Continuity Plan in place covering personal computers and servers.
- If credit union uses an outsource contractor to provide all or part of its IT support function, an outsourcing agreement is in place providing adequate detail on the scope of the services covered by the agreement.

2.25 NEW CUSTOMER-OWNER APPLICATION AND IDENTIFICATION

Internal Control Objective:

To ensure the credit union has implemented appropriate procedures to support new customer-owner applications and to ensure the requirements of privacy legislation and money laundering legislation for new account openings are met.

Best Practice:

- Latest version of application forms provided by CUCNS for Personal and for Business accounts or in-house developed forms that are similar in content used by the credit union.
- Application and signature card fully and properly completed, signed by the customer-owner(s) and witnessed, preferably by a credit union staff member, and initialled by staff. Other documentation required for business membership and account openings fully completed and signed as required.
- Minimum one, preferred two, references listed on the application.
- Details recorded on the application from at least one valid piece of identification but preferably two of which one is a photo ID.
- Identity confirmed in accordance with FINTRAC guidelines.

Note - refer to FINTRAC Guideline 6G – Record Keeping and Client Identification for Financial Entities.

- Credit report obtained and attached to the application, especially if the person is unknown. Applicant authorization provided in writing to allow the credit union to perform a credit check.
- Appropriate ICU, ATM and POS limits established consistent with credit union policy.
- All new account openings checked to the CUCNS Fraud Warning System.
- New customer-owner account opening practices meet all requirements outlined under FINTRAC guidelines.
- Applications and signature cards filed / maintained in secure manner.
- New accounts monitored (for large or unusual number of deposits, returned clearing items, overdrafts, non-branch transaction greater than \$2,500, change of address requests, returned mail, frequent ATM withdrawals, cheques issued by the customer-owner from another financial institution, ICU transactions, etc.).

2.26 CLEARING

Internal Control Objective:

To ensure the appropriate processes and controls over daily clearing items are in place.

Best Practice:

- To meet the CPA guidelines, appropriate action taken within the required time to return clearing items that contain errors.

- Non-posted cheques, direct deposits, and pre-authorized debits investigated and corrective action taken to post or return individual items and associated internal accounts are cleared.
- NSF items to be accepted and posted to the customer-owner accounts properly authorized by the appropriate authority level and evidence of approval documented.
- Tellers set up for clearing transactions balanced daily.
- Unqualified items reviewed and investigated and appropriate entries made daily. Necessary offsetting entries made daily to the credit union's current account.
- Supervisory review of daily balancing reports, internal accounts, etc. at least once a week on a random basis.

2.27 INACTIVE ACCOUNTS AND DORMANT ACCOUNTS, AND UNCLAIMED BALANCES

Internal Control Objective:

To ensure appropriate controls and regulatory compliance are in place for the management and administration of Inactive and Dormant Accounts, and Unclaimed Balances.

Best Practice:

- Inactive Accounts/Unclaimed Balances Policy (Capital Procurement Section 23000, Sub-section 23300 Rev Dec-05) approved by the Board of Directors.
- Procedure similar to Operating Guidelines 8000 - Inactive, Dormant & Unclaimed Balances - revised Dec-05 implemented to identify, properly control, administer and monitor inactive, dormant and unclaimed balance accounts.
- Clear and permanent records kept on all inactive and dormant accounts so that future claims by the customer-owner may be handled efficiently. Also, to ensure once the accounts reach the "unclaimed" status they may be handled in a manner consistent with current credit union legislation.
- Membership Activity Monitoring Report 335-1 compared to previous month report to determine and investigate accounts no longer being reported. Attempts made to reactivate accounts and follow-up activity documented. Report reviewed by management monthly.
- MemberDirect Cards blocked and POS, ATM, ICU limits cancelled on accounts identified as inactive, dormant or unclaimed until customer-owner contacted and/or decision made to reactivate or close account.
- Supervision and management authorization of account reactivation. Tellers do not have the ability to process a transaction on an inactive account without a supervisory override.
- Procedure in place to monitor transactions processed on inactive accounts (e.g. Daily Report 319-2 Transactions of Note – Management review daily).
- The general manager or his/her designate, and one other employee (normally the teller) each initial all vouchers with respect to transactions processed on inactive and dormant accounts. Proper identification obtained from the customer-owner for withdrawals and the signature compared to the signature card on file.

- When accounts have been closed by the credit union, a printout of the account showing the closing balance taken and held in a separate file in safekeeping under joint custody. Signature card pulled and attached to the printout for filing, and a dummy signature card produced to replace it and indicates “inactive account – closed to service charges” or “unclaimed balance – transferred to CUDIC”, whatever the circumstances.

2.28 STAFF MEMBER ACCOUNTS, LOAN & CREDIT FILES AND PRIVACY CONSENTS

Internal Control Objective:

To ensure the credit union has an appropriate process to monitor staff accounts for unusual or inappropriate transactions and to provide security and confidentiality of staff loans and personal information.

Best Practice:

- Clearly defined policy and process in place for the approval and administration of staff loans.
- Employees advised in writing that as part of prudent credit union internal control practices, personal accounts are subject to monitoring and review. Each employee signs an Employee Privacy Consent. A Privacy Consent (Joint Account Holder with Employee) also signed by the joint account holder if the staff has a joint account with another individual.
- The General Manager or designate periodically review staff accounts (preferably monthly) for unusual transactions to confirm all staff members operate their accounts in a satisfactory manner and that all transactions are in the normal course of business.
- Perusal of the General Manager’s accounts completed by the Audit Committee, Executive of the Board or designated senior staff provided with the ability to report any derogatory findings directly to the Board.
- Employees formally advised and acknowledge in writing they are not permitted to process transactions for self, immediate family members, businesses involved at arms length with, and organizations where they are part of the executive or have signing authority on the accounts.
- For security and confidentiality reasons, all staff loan and line of credit account files kept separate from the regular customer-owner files and kept in a secure location under the sole custody of management or designate.

2.29 PROFESSIONAL CONDUCT, CONFIDENTIALITY AGREEMENT & CONFLICT OF INTEREST DISCLOSURE

Internal Control Objective:

To ensure the credit union has implemented appropriate policies and procedures for confidentiality and conflict of interest for employees, board and committee members.

Best Practice:

- Standards of Professional Conduct Policy 5000 approved by credit union Board. Policy includes the credit union’s Code of Business Conduct, Confidentiality Agreement and Conflict of Interest Policies.

- Board, committee and staff members required annually to acknowledge the Code of Conduct and sign a Confidentiality Agreement and Conflict of Interest Disclosure / Statement of Disclosure Agreement.
- Report provided to board or designated committee (e.g. Audit and Conduct Committee) confirming all Directors, Committee members and employees signed the applicable Code of Business Conduct Agreement, Confidentiality Agreement and Conflict of Interest Agreement, and identification of any exceptions, and expected resolution.
- Integrity in Action program (CUMIS) adopted by Board and Management.
- Fraud/Dishonesty Policy and Procedures 7060 approved by the Board and procedures implemented. Fraud/Dishonesty Policy Statement signed at least annually by all employees.
- Mandatory two-week uninterrupted vacation requirement / policy for staff approved by the Board.

2.30 MANAGEMENT, STAFF, BOARD AND COMMITTEE EXPENSES

Internal Control Objective:

To ensure appropriate control and management for settlement of employee, board and committee expenses.

Best Practice:

- Board approved policy, which adequately regulates management, staff, board and committee member expenses (travel, meeting, conference, education, parking, etc.).

Note: This is normally established under Board of Directors Policy Section 11000, Remuneration and Expense Subsection 11175(3), Training, Education and Development Subsection 11600(3), and Personnel Policy Section 15000, Expense Accounts (staff) Subsection 15175.

- If corporate expense cards are issued, Board approved policy regulating the use of corporate cards for expense payments. Policy and operating guidelines acknowledged in writing by holders of corporate cards.
- Policies indicate eligible and ineligible expense and reporting requirements including timeframe within which a report must be submitted for settlement of claims and cash advances, standard rates (e.g. per diems, use of personal car rates, etc.), supporting documentation requirements, authority levels for approvals, grievance resolution process, etc.
- Standardized consistent reporting format for expense claims used within the credit union (form, receipts, details, etc.).
- Accountability evident in the processing of expense claims, that is, the claimant, person with approval authority and preferably also the person auditing the report duly sign the expense report before settlement is made.
- Only original receipts / invoices considered for payment.
- Copy of the voucher(s), the documented settlement date, where and how settlement/funds (i.e., expense GL #s and/or accounts) disbursed, documented and attached to the expense report unless an area on the report has been designated for the entry of this information.

- All vouchers in support of the claim marked “Paid” and the payment date recorded and receipts / invoices attached to the claim form.
- Audit Committee or Board designated Committee performs a periodic review of travel expense reports and expenditures to ensure all made within policy.

2.31 CREDIT UNION OPERATING EXPENSES

Internal Control Objective:

To ensure appropriate control and management for settlement of credit union operating expenses.

Best Practice:

- Board approved policy, Authorizations (corporate expenditures) Subsection 11250(2).
- Invoices/receipts for expenses authorized for payment by the required approval authority as established by policy.
- Only original receipts / invoices considered for payment. Once settlement is made, receipt / invoice marked “Paid”.
- All invoices/receipts provide evidence of approval for settlement, settlement date, where and how settlement/funds (i.e., expense GL #s and/or accounts) were disbursed.

2.32 REPORTING TO THE BOARD OF DIRECTORS

Internal Control Objective:

To ensure the Board of Directors and its committees are receiving appropriate reporting / information to make informed decisions in meeting their corporate governance responsibilities. Also, to ensure they are meeting the requirements as defined in legislation and in the by-laws of the credit union.

Best Practice:

- As outlined in the Credit Union Board of Directors Handbook, board reporting includes:
 - Manager’s Report
 - Committee Reports (Credit, Audit, Executive, Personnel, Property, Marketing, etc.)
 - Correspondence
 - Old and New Business
- Manager’s Report to the Board:
 - The written part includes:
 - Corporate Governance
 - Numbers of New and Closed Customer-owners and comments
 - Board/Committee Members – comments
 - Personnel – comments
 - Community – comments
 - Information on ALM as per the credit union’s policy (minimum quarterly)
 - Development – comments on planning, service and product development, marketing, technology, district, provincial and national issues, etc.

- Privacy of Information
- Money Laundering
- The financial part includes:
 - Financial Monitoring Overview – actual figures – previous year-end to current month
 - Financial Overview – actual to budget and variances
 - Financial Report – actual net figures monthly for the year
 - Investment Report – quality, terms, maturity, returns/interest rate and accrued interest
 - Liquidity Monitoring Report – cash flow, comparisons, etc.
 - Written comments on key areas, notable variances, significant changes, etc.
 - Current Interest Rate Sheets with comments on rate changes in the month.
 - Loan portfolio mix and comparison by quarter.
- The Credit Committee’s report to the board includes:
 - Overdrafts – comparisons
 - Delinquency – comparisons
 - Loans / Lines of Credit – portfolio mix, activity, authorized
 - Exceptions to Policy
 - Allowance for Impaired Loans (minimum quarterly)
 - Credit Committee meeting minutes.
- The Audit Committee’s report to the board includes:
 - Recommendations to the board regarding the selection process for the external auditor, the appointment of the auditor, and the terms of engagement of the auditor (annually). Also to include recommendations regarding the reports and recommendations made by the auditor.
 - Report on adherence by directors and officers of the credit union to the requirements of Section 96 of the Act (i.e., interest in “material contract” - minimum annually).
 - Report covering its review and ongoing monitoring and progress of actions being taken to implement recommendations of all reports on the affairs of the credit union made by the Superintendent or CUDIC, or any report referred to it by the board (ongoing).
 - Report covering the committee’s review and/or development of policies or other duties as directed by the board (ongoing).
 - Audit Committee meeting minutes.

2.33 MEETING AGENDAS

Internal Control Objective:

To ensure the Board of Directors and its committees are provided with a clear agenda of the items to be considered in an orderly fashion at the meeting and to determine any conflicts of interest prior to the start of the discussion on the listed agenda items.

Best Practice:

- Meeting agendas established for each specific meeting of Board of Director, Audit Committee, Credit Committee and other committees of the board.
- Board meeting agenda includes attendance, call to order, roll call (to establish quorum), review of agenda, call for any conflicts of interest, minutes of last meeting(s), manager’s report, financial reports, membership report, committee reports (credit, audit, executive, policy, personnel, property, marketing, human resource, etc.), old business, bring forward list, correspondence, new business, in camera (as required), date of next meeting, and adjournment.

- Committee meeting agenda to include, as a minimum, review of agenda, call for conflicts of interest, minutes of last meeting(s), reports, old business, bring forward list, correspondence, new business, date of next meeting and adjournment.

2.34 RECORDING OF MEETING MINUTES

Internal Control Objective:

To ensure the recorded minutes properly reflect the proceedings, correspondence, reports reviewed, discussions, and decisions made. Also to ensure the safeguard of the information provided and minutes as archives of the credit union.

Best Practice:

- Appropriate minutes of Board and Committee meetings recorded and maintained in an organized fashion. The minutes and respective correspondence, information and reports are credit union archives to be appropriately secured and held in the credit union vault / safe.
- Minutes of the Board of Directors reflect / include:
 - review of the agenda and any changes made;
 - evidence of call for and recording of any conflict of interest or no conflicts declared;
 - motion to approve the minutes of the previous meeting(s) including the dates of the previous minutes and reports being approved by the motion (note – if changes were made to the minutes of meetings, those changes must be initialled by the Secretary and Chair);
 - details / comments on discussions that took place on various issues/agenda items leading to decisions/motions;
 - motions in minutes identify the month for which reports (Manager's Report, Financial and Progress Reports, Liquidity Reports, ALM Reports, Investment Reports, Allowance for Impaired Accounts Report, Write-offs, etc.) are being reviewed and approved. This keeps track of the reports the Board or Committee have been presented with and considered.
 - motions recorded in the Board meeting minutes dealing with exceptions to Loan Policy clearly indicate the policy/limit affected by the exception, the description of the exception with the extent it is exceeding the policy limit, the account number and loan amount. A copy of the completed exception request form attached to the minutes for reference.

Note - It is at the Board's discretion if they wish to have the names identified in the motion. If the Board has appointed an Exception Committee to approve exceptions, the committee reports to the Board at the next meeting and the Board's motion should indicate the exception was ratified rather than approved;

- initials of the recording secretary and president / chair on all pages of minutes and their signatures on the final page once the minutes have been formally approved by the board. If changes made to the minutes, initials of the Chair and Secretary / Recorder by the changes; and
- a copy of all reports, revised/new policies approved, correspondence, etc. dealt with at the Board meetings attached to the minutes.

- Minutes of the Committees reflect / include:
 - evidence in credit committee minutes that it is meeting all of its requirements under Regulation Section 27 of the *Credit Union Act* and the By-laws and policies of the credit union;
 - evidence in audit committee minutes that it is meeting all of its requirements under Regulation Section 26 of the *Credit Union Act* and the By-laws and policies of the credit union;
 - evidence that the minutes of all committees include:
 - review of the agenda and any changes made;
 - evidence of call for and recording of any conflict of interest or no conflicts declared;
 - motion to approve the minutes of the previous meeting(s) including the dates of the previous minutes and reports being approved by the motion (note – if changes were made to the minutes of meetings, those changes must be initialled by the Secretary and Chair);
 - details / comments on discussions that took place on various issues/agenda items leading to decisions/motions;
 - initials of the recording secretary and president / chair on all pages of minutes and their signatures on the final page once the minutes have been formally approved by the committee; and
 - copy of each report, etc. dealt with at the committee meetings attached to the minutes.

2.35 MONEY LAUNDERING REGIME AND COMPLIANCE

Internal Control Objective:

Credit union compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), Regulations, and Operating Guidelines provided by the Financial Transaction Report Analysis Center of Canada (FINTRAC).

Best Practice:

- Adherence to the requirements of the *Proceeds of Crime and Terrorist Financing Act*, the Regulations and the Operating Guidelines provided by FINTRAC including the implementation of a full compliance regime, meeting the record keeping and retention of information requirements, and reporting to FINTRAC as required.
- Use of standard Money Laundering policy, procedures, forms and documents developed and distributed by CUCNS.
- Evidence that appropriate action taken to address any previous non-compliance issues identified by regulators, auditors or previous internal compliance reviews.

2.36 DELEGATION OF LENDING LIMITS & DISBURSAL OF LOANS

Internal Control Objective:

To ensure appropriate segregation of duties and approval authority exist in lending.

Best Practice:

Delegation of Lending Limits

- Lending and overdraft approval limits clearly stated and designated in writing to each individual lending staff by the appropriate authority. When limits further delegated to more junior staff, person delegating received authority to do so in writing from the General Manager or President & CEO prior to making any such delegations.
- Individual lenders acknowledgement in writing indicating the Capital Utilization Policy and designated limits were received, read, and understood. Signed acknowledgement and designated limits are kept in a secure location by the General Manager or designate. A copy of designated limits and acknowledgement provided to the lender for personal reference.

Disbursal of Loans

- Segregation of duties and accountability evident.
- Consistent practices and procedures amongst the credit union branches followed for the disbursal of loan proceeds. This includes the vouchers or disbursal document/form used for the disbursal.
- All disbursals of loan proceeds done through a loans clerk or front-line tellers not associated with lending. Staff member processing the disbursal does not have the ability to enter/post the transaction without a supervisor override.
- CEO / General Manager and/or Senior Lending officers review the listing of new and renewed loans, lines of credits, and mortgages approved and advanced each month to ensure all loans over lenders individual limits were appropriately approved in accordance with policy.

2.37 PROTECTION OF PERSONAL INFORMATION

Internal Control Objective:

To confirm compliance with the Protection of Personal Information and Electronic Documents Act. (PIPEDA)

Best Practice:

- Board approved policy for the protection of personal information that covers the ten privacy principles of the Personal Information and Electronic Documents Act. (Policy section 5700 - Protection of Personal Information and Credit Union Code for the Protection of Personal Information)
- Appointment of a Privacy Officer by a motion of the Board of Directors and documented in the minutes of the board meeting. Appointment documents privacy officer's responsibility, authority and accountability for ensuring compliance with the privacy legislation and the credit union's privacy policy.
- Through the General Manager, Board of Director's designation of a replacement Privacy Officer who will be available in the event of absences of the Privacy Officer and who will have the same responsibilities of the Privacy Officer.
- A self assessment compliance program completed at least annually, including reporting self assessment results at least annually together with recommendations provided by the Privacy Officer to senior management and the Board of Directors within four months of each calendar year end.

- Ongoing process in place to monitor, assess and address the effect on privacy from changes made to operations, staffing, technology, laws, regulations and contracts.
- All complaints and inquiries reviewed by the Privacy Officer and response and action taken assessed for appropriateness.
- Ongoing compliance training / education program in place for employees and Board members.
- Appropriate application and consent forms used consistent with the requirements of the Personal Information and Electronic Documents Act.
- Legal agreements in place with third parties to support the receiving and/or sharing of personal information.
- Information on credit union's privacy policies readily accessible to external parties.
- Appropriate action taken to address any previous non-compliance issues identified by regulators, auditors or previous internal compliance reviews.

2.38 POS, ATM AND ICU LIMITS, MEMBERCARDS AND CONTROLS

Internal Control Objective:

To ensure the assignment and monitoring of individual card limits to customer-owners is appropriately managed and controlled.

Best Practice:

- Standard limits established by credit union for POS, ATM and ICU limits.
- Formal request made in writing by customer-owner for card limits.
- System in place to ensure temporary increases requested by the customer-owner are reduced on a timely basis.
- For permanent increases requested by the customer-owner, the credit union to obtain a formal request and authorization from the customer-owner for the increase. Customer-owners are formally advised of the increased risks associated with higher limits and confirm to the credit union in writing their understanding of the risk to them especially should their PIN be compromised.
- Limits not provided on cards that access accounts where two signatures are required on withdrawals.
- No limits attached to credit union internal accounts.