MITIGATING THE RISK OF INTERNAL FRAUD

MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

INTERNAL FRAUD RISK CONTROL WORKING GROUP

JUNE 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

Two significant, longstanding frauds were exposed recently in Michigan, causing Boards and senior managers at credit unions around the state to evaluate their current fraud mitigation practices.

In the case of Shoreline Federal CU, a $17 million dollar West Michigan Credit Union, the CEO embezzled $2 million by both stuffing cash from the vault in her purse and depositing stolen funds into her own and family member accounts a total of 433 times over a period of 17 years. She hid her embezzlement from auditors and supervisory committee members by manipulating financial statements to make it appear that the missing cash was on deposit at the credit union's correspondent bank.

And in early 2016, we learned that the CFO at the $66 million Clarkston-Brandon Community CU had embezzled more than $20 million over a period of a dozen years. The CFO transferred large sums of money to his personal accounts at various financial service providers. Reportedly, the CFO was creating phony documents purporting to show investments held by the credit union. The fraud rendered the credit union insolvent which resulted into the credit union being placed into conservatorship, and it was recently merged into another credit union.

The taskforce was established to identify and evaluate what types of internal controls and fraud prevention policies, procedures and tools are in place as well as identify what credit unions are doing— and should be doing— to address issues of insider fraud, based on size and complexity.

The taskforce focused on developing best practices and industry norms for internal controls and fraud prevention, specifically examining segregation of duties among staff, supervisory committee oversight, internal controls/internal audit oversight, and the responsibility of the Board of Directors.

PROCESS

Member Survey: Prior to beginning the work of the taskforce, MCUL conducted a survey of Michigan Credit Unions designed to gather feedback on the fraud control and risk mitigation efforts currently in use by the member institutions. A short version of the results of this survey can be found in Appendix A of this report. Complete results can be found at http://www.mcul.org/regulatory-outreach

Taskforce Members: We want to thank the taskforce members for generously volunteering both time and expertise to this project. We had excellent speakers, robust discussion and a candid examination of a series of key factors at play in the Michigan credit union community today.

Jessica Broad, NCCO	Compliance Officer|Gerber Federal CU
Tim Donnelly, CUCE	Compliance and Risk Management Specialist|Dow Chemical Employees CU
Robin Hoag, CPA	Shareholder and Practice Leader|Financial Institutions Group
	Doeren Mayhew, CPAs and Advisors
Chuck Holzman, J.D.	Managing Partner|Holzman Corkery, PLLC
Jim Hunsanger, CPA	Vice President, Internal Audit|Michigan State University Federal CU
Tom Kuslikis, CPA	Vice President of Accounting and Finance|University of Michigan CU
Triston Kirt	Compliance & Security Officer|TBA CU
Dan Mahalak, CPA	President and Managing Partner|Cindrich, Mahalak & Co.P.C.
Catherine Morey, CFCI	Vice President, Risk Management|Alliance Catholic CU
Ken Ross, Chair	EVP/COO|Michigan Credit Union League & Affiliates
Sarah Stevenson,CUCE	Senior Regulatory & Legislative Affairs Specialist|MCUL
Jack Tracy, CPA	Shareholder|Financial Institutions Group|Doeren Mayhew|CPAs and Advisors

Meetings: The taskforce met three times during the period of March 2016 through May 2016 and heard the perspectives of a wide variety of experts including:

Meeting 1 Topic: Recent cases of fraud in depositories, root causes and key findings.

Speakers

Dan Mahalak, CPA	President and Managing Partner|Cindrich, Mahalak & Co. P.C.
Robin Hoag, CPA	Shareholder and Practice Leader|Financial Institutions Group
	Doeren Mayhew, CPAs and Advisors
Jack Tracy, CPA	Shareholder|Financial Institutions Group|Doeren Mayhew|
	CPAs and Advisors
Chuck Holzman, J.D.	Managing Partner|Holzman Corkery, PLLC

Meeting 2 Topic: Regulatory perspectives on credit union internal fraud risk.

Speakers

LeAnne O'Brien	Assistant Director|Office of Credit Unions|DIFS
D. Scott Neat	Director|Division of Supervision|Office of Examination and Insurance|NCUA
JeanMarie Komyathy	Director of Risk Management|Office of Examination and Insurance|NCUA

Meeting 3 Topic: Fraud detection and prevention.

Speakers

Rob Pilch	Risk Consultant|Business Protection Risk Management|CUNA Mutual Group
Bryan Callahan	Director|Forensics and Valuation Services|BKD, LLP

RECOMMENDATIONS

After reviewing recent incidents of fraud losses at credit unions; exploring lessons learned from specialists that focus on credit union regulation and fraud mitigation; reviewing common fraud prevention techniques currently employed in Michigan credit unions today; and utilizing available risk assessment models, the task force developed this white paper.

Credit union management and Boards are encouraged to:

- Familiarize yourselves with the case capsules describing recent frauds perpetrated
- Review the internal fraud prevention safeguards and internal controls and determine which are appropriate for your credit union and how they can be implemented given your size and risk profile
- Using the template provided, or one of your own design, conduct a risk assessment, which you should review and update periodically
- Review the fraud prevention survey results and identify any gaps in your current risk mitigation environment
- Consider whether you need to periodically invest in having an independent 3rd party, such as your external auditor, to conduct an expanded scope audit designed to test internal controls
- Have the Board adopt a fraud policy. A model policy is provided in the Appendices to this white paper.
- Have the Chairman of the Board and CEO sign the attached Statement of Commitment
- Provide training to staff on internal fraud red flags, fraud prevention policies and procedures, and whistleblower protection laws
- Encourage credit union staff and volunteers to call the toll-free hotline to report suspected fraud

INTERNAL FRAUD PREVENTION

OVERVIEW: SAFEGUARDS AND INTERNAL CONTROLS FOR CREDIT UNIONS

Banks and credit unions face both internal and external fraud risk. To mitigate these risks, credit unions need a strong and effective system of internal controls to operate in a safe and sound manner. A primary objective of effective internal controls is to prevent misappropriation of funds. In an effort to assist credit unions in mitigating fraud, the taskforce compiled a list of the following internal controls for credit unions to consider implementing.

Provided first is a series of more generalized internal controls recommended for all credit unions to adopt. This white paper is then broken down into internal controls by operational area. The document is intended to provide recommended best practices to assist credit unions in combatting the risk of internal fraud and should of course be scaled based on staffing, size and complexity among each institution. This document should not be considered as an all-inclusive list of internal controls or best practices.

Internal Controls for all Credit Unions

- Hotline
  The number one way that fraud is detected is through tips. Promotion of a whistleblower hotline credit union employees and volunteers could anonymously call if they suspect fraud would be an important means for curtailing fraud once detected.
- Compulsory Vacations
  A compulsory, consecutive one- to two-week vacation forces individuals to relinquish their duties to someone else, allowing the potential for irregularities to surface. A policy for compulsory vacations is only effective if someone else can transition to the position while the employee is gone and remote access is blocked during vacation.
- Written Fraud Policy
  Together with legal counsel, credit unions should develop a written fraud policy including oversight by management, senior executives and Board oversight. The policy should also include employee responsibilities and potentially a fraud policy agreement for staff to sign annually.
- Appropriate Training At All Levels
  A credit union can have the best fraud policy in the world but without proper training it is unlikely to be effective. Conducting fraud awareness training for all employees, management and the Board of Directors to ensure everyone understands how fraud can be detected is critical.
- Annual Independent Audit
  Contracting with a Certified Public Accounting (CPA) for an annual independent audit ensures examination of all risk areas, with those of the greatest risk receiving priority.
- Annual Independent Account Verification
  Contract with a CPA as part of the annual independent audit process, or an independent third party, to conduct an independent account verification of the credit union's accounts (e.g., Certificates, Lines of Credit, and all other investment accounts.) Verification of this nature will aid in identification of any discrepancies between reports and balance sheets provided by credit union management and external account records.
- Biennial Internal Controls (Expanded Scope) Audit
  Conducting an independent audit of the credit union's internal controls, at a minimum, every other

year, can provide reasonable assurance that internal controls are functioning properly in order to safeguard the assets of the credit union as well as prevent and detect errors and irregularities that may otherwise go undetected during a routine audit. An expanded scope audit would be in addition to the credit union's annual financial audit.

- Board Oversight
  Credit Union Boards should have oversight of the credit union's anti-fraud program. The Board should also be meeting with examination staff and auditors on a regular basis. Internal controls need to be implemented at the Board level and established throughout the credit union. Additionally, the Board should ensure appropriate follow-up on examination and audit findings.
- Segregation of Duties
  Segregation of duties can be difficult when staffing is limited, however fraud can be significantly limited if appropriate segregation is in place. Most transactions can be broken down into the following three steps: processing, approval, and funding. One employee should not have complete control over all steps within a transaction.
- Rotation of Duties
  This can also be a difficult task when staffing is limited, however rotation of duties has both internal control benefits as well as cross-training benefits. Cross-training provides for staffing when an employee goes on vacation and can also aid in identification of irregularities. Additionally, rotation of duties supports a credit union's Contingency and Recovery Planning program and process.
- Appropriate Dual Controls In Place
  Dual controls over vault cash, wire transfer functions, and various other functions provide oversight and deterrence of fraud. Another set of eyes on a transaction can shed light on potential irregularities. Access should be limited based on job function; i.e., limiting who can access what.

Internal Controls by Operational Area

Accounting

- Compulsory vacations – cross-training of staff to handle duties while on vacation
- Directors and Management review financial reports and statements
- Independent direct verification of Fed and Corporate Accounts
- CFO and CEO review general ledger account variances on a monthly basis
- Internal and External Auditors perform a review of manual journal entries on a periodic basis
- Reconcilement of all balance sheet accounts on a monthly basis
  - Outstanding items reported to appropriate area
- Require management approval on all Accounts Payable checks prior to issuance in accordance with purchasing policy
- CFO should not have access to create invoices or issue checks
- Segregation of duties in Accounts Payable process
- Corporate Procurement Card Policy
- Limitation of user control and access to General Ledger (GL)

Wire Transfers

- Ensure adequate segregation of duties between employees who can approve a wire request and those that can process the wire request
- Wire transfers are settled through correspondent bank accounts, and these should be reconciled on a daily basis and confirmed annually by independent auditors
- Access to the Federal Reserve System granted by the CFO, however CFO should be able to only make changes to user and institution settings; and should not be able to transfer funds
- Wire transactions over an internally set threshold require dual verification

Correspondent Bank Accounts

- Accounting Department reconcilement of Federal Reserve Account daily
- Individuals not responsible for posting transactions to correspondent bank accounts reconcile each account monthly
- Several individuals monitor all correspondent bank account balances throughout each week to ensure there are sufficient funds to cover settlements, purchase investments, make payments, etc.
- Internal Audit conduct audits of account reconciliations annually at a minimum
- External Audit independently confirms correspondent bank accounts directly with the institution of record annually

Cash and New Account Operations

- Verification of bulk currency under dual control
- Dual Control for vault access
- Surprise cash counts
- Over/Short records maintained
- Employees restricted from transactions or maintenance of their own account(s) and accounts of family members
- New accounts opened by individuals who do not process or approve loans
- Member Service Representatives buy and sell cash drawers at the beginning and end of their shifts.
  - Each is tracked by the employee number of the employee handling drawer
  - Establishes ownership and allows for efficient audits
- Branch(es) perform nightly balances, and any differences are investigated
  - Employees involved in any discrepancy cannot leave until discrepancy is determined
- Management investigation of over/short general ledger postings
- Branch(es) perform their own monthly and quarterly surprise audits
- Internal Audit or Supervisory Committee conduct quarterly surprise audits at each branch
- Cameras in place throughout all cash-handling areas
- Cash ordering privileges are assigned by management
  - Orders reviewed daily through the Federal Reserve reconcilement
- Cash orders can only be delivered to branches and ATM servicer locations as documented with Federal Reserve
- Periodic review of accounts coded as “No-Mail”

Lending

- Segregation of duties – Process/Approval/Funding of loans
- Lenders have no or limited ability to open accounts
- Internal Audit or Supervisory Committee performs independent audits over all loan types on a monthly or quarterly basis
- External audit and regulators audit an additional sample of loans at least annually
  - Include confirmation of outstanding balances for a sample of members
- Internal Audit or Supervisory Committee conduct the following reviews over loans in an effort to identify potential fraud:
  - Accounts with a mailing address at the credit union (monthly)
  - Loans with due dates greater than 120 days in the future (monthly)
  - Loans with interest accrued over $1,000 (monthly)
  - Addresses or SSNs with more than 10 loans (periodically)
  - Loan and account file maintenance changes (daily)
  - Dormant account activity and confirmation of such (weekly)
  - Loans funded by lender who approved applications (monthly)
  - Transaction activity in test accounts used by the credit union (monthly)
- Validation on key input data – restricting access to the data to certain users
- Periodic review of accounts coded as "No-Mail"

Collections

- Review of File Maintenance Reports
- Review of Loans in a Paid Ahead Status – advanced due date
- Review of General Ledgers for payments on charged off loans

Electronic/Data Processing

- Access Levels (permissions)– core processing system
  - Implement principle of least privilege, ensuring access and permissions are limited and aligned with employee job functions/roles
- Password Protection – passwords changed regularly
- Security Policy
- Review of Supervisory override reports
- Review of Dormant/Inactive Account overrides
- Review of File Maintenance Reports
- Access to post general ledger entries is restricted by position.
- CFO does not have access to post entries to the general ledger system.
- Review of changes to access levels
- Periodic review of access controls to ensure that they are still appropriate

Investments

- Board-approved investment brokers are the only individuals authorized to perform investment purchases and sales
- Only the Credit Union can purchase Board-approved investment vehicles
- Investments settled through correspondent bank accounts are reconciled on a daily basis and confirmed annually by independent auditors
- Investment safekeeping (custody of the actual investment) performed by a third-party
- Internal Audit audits investment purchases and sales at least annually, compare the investment accounting reports to the safekeeping reports and correspondent bank records.
- Annually, external auditors independently confirm investments directly with the safe keeper
- Funds for investment purchases are wired to the appropriate account based on wire templates that cannot be updated by any of the Accounting and Finance employees, including CFO

Business Owned Life Insurance (BOLI)/Deferred Compensation Arrangements

- Only Board-approved insurance brokers are authorized to perform such transactions
- Transactions settle through correspondent bank accounts, which are reconciled on a daily basis and confirmed annually by independent auditors
- External auditors independently confirm BOLI and Deferred Compensation policies directly with providers

Employee Accountability

- Internal Audit/Management conducts regular monitoring of employee account activity with respect to:
  - Courtesy Pay usage
  - Non-Sufficient Fund activity
  - Balances extending beyond credit limit
  - Delinquent loan payments
  - Overdrawn accounts
  - Suspected check kiting
  - Possible suspicious account activity recognized by our BSA software, identifying employees experiencing financial hardships and who may be more susceptible to embezzlement
- Employees are not allowed to post transactions to their own accounts.
- Financial Responsibility Training for employees
- A Board adopted Financial Responsibility Policy
- Whistleblower Hotline – Distribute information to all employees and Board of Directors and post in break/lunch room

Appendix A – Specific Examples of Fraud

BACKGROUND

As part of its information gathering, the task force heard from CPA's, attorneys and state and federal regulators, who recounted specific incidents of fraud that they had encountered in the course of their professional careers. Both shortcomings in credit union risk mitigation programs, and in some cases, the ability of key employees to evade detection by falsifying records and exploiting internal control weaknesses, were identified and discussed at length.

Because some credit union professionals have raised concern that there hasn't been sufficient transparency regarding the specific ways in which frauds are being perpetrated against credit unions, we provide several examples of "what actually happened" when fraud was detected.

CASE CAPSULES

Credit Union #1

$100mm credit union | $1.3mm loss

The fraud occurred from 1993-2006 and was uncovered in May 2006. The fraud was perpetrated by a long term and trusted employee of the credit union, the Loan Supervisor. This individual created 58 fictitious member and loan accounts with 216,000 transactions taking place over a 13-year period. The total loss to the credit union added up to $1.6mm. The control systems in place were very weak, allowing the fraud to occur over this long period of time. The scheme finally collapsed when a mailer went out and was returned bad address, triggering an investigation

Control weaknesses

- **Segregation of Duties**: Employee could open accounts, make file maintenance changes, process and approve loans as well as fund loans. Once the loans were created and funded this individual could set up a home banking link to move money between accounts that never required human intervention.
- **Inadequate file review:** This individual forged credit committee signatures as well as altering loan documents. This individual would also flag accounts to indicate "No Mail to Member."

Credit Union #2

$150mm credit union | $317,000 loss

The fraud occurred over the course of six years, from 2006-2012, and involved a long-term employee, a senior teller, taking money from the vault. The teller had access to post to general ledger accounts and knew when the surprise cash counts were going to be conducted. The individual would make journal entries in the GL to cover up the amount she had stolen, prior to the cash count, to cover any discrepancy that would have surfaced had she not manipulated the GL. The individual also knew when the corporate account GL was reconciled and would falsify corporate credit union documents as well. Over the course of six years this individual embezzled $317,000. The scheme was finally caught when the teller was transferred to another branch. While controls were in place, such as the surprise cash counts, they were too routine and predictable.

Control weaknesses

- **No Surprises**: The teller had access to post to general ledger accounts and knew when the surprise cash counts were going to be conducted.
- **GL Reconciliations**: Daily or weekly general ledger reconciliations on the primary corporate bank account would have assisted in identifying the fraud sooner.

- Compulsory Vacation: Consecutive one- to two-week vacation, with another employee assuming responsibilities was not in place or enforced.

Credit Union #3
$45,000 loss

$45,000 stolen over the course of six to seven months from the credit union's own ATMs and perpetrated by one individual. One employee would count the $20s and the other would count the $10s. The individual counting the $20s would steal funds and because the credit union serviced their own ATMs, while dual control was in place for counting the cash, the employees did not rotate duties. The employee counting the $10s never questioned the other individual's process.

Control weaknesses

- Dual controls existed but were subverted by staff: The controls were established correctly but were not effectively being executed.

Credit Union #4
$320,000 loss

$320,000 loss to the credit union. Perpetrated by a long term, 40-year employee, who had control over the vault and was stealing vault cash. This employee would steal $100 bills from bill packs and replace the missing bills with $1 bills leaving a $100 bill on the top and bottom of the packs. When the vault was audited the bill packets were never broken down so it always looked like the appropriate amount of cash was in the vault. The employee's scheme was finally caught when an audit of the vault was conducted in which the bill packs were broken down.

Control weaknesses

- Vault cash never counted: The vault cash was never rotated or opened.

Credit Union #5
$86,000 loss

Information Technology Staff had too much administrative coding ability. The staff could make changes to account balances and made changes totaling over $86,000. The staff could restore balances and transfer money out of the credit union all by electronic means. The scheme was finally caught when a balancing review was conducted. It took an extensive investigation including the use of cameras and mirroring to determine the full extent of the scheme.

Control weaknesses

- Segregation of Duties: There was not a good change management process for coding changes. Any changes to system coding should be approved by someone other than the individual that made/implemented the coding change.

Credit Union #6
Shoreline Federal Credit Union | $2mm loss

$2mm loss to the credit union. This case involved a long-term, trusted CEO of a small credit union. The CEO had embezzled funds from the credit union since 1998. She removed cash from the vault on 433 separate occasions and covered the thefts by falsely reporting that the money had been transferred to the credit union's corporate

account. Discrepancies uncovered during a routine external audit in 2015 resulted in additional follow up with the credit union's corporate credit union, and an overstatement in the credit union's general ledger of nearly $2mm was detected. Upon identification of this discrepancy and upon further investigation by the auditors and the federal regulator the CEO's embezzlement scheme collapsed.

Control weaknesses

- **Segregation of Duties:** The CEO had complete control over all records and vault cash.
- **No surprises:** Credit union controls were minimal and trust was placed in the CEO. Due to this misplaced trust, no true "surprise" audits were conducted.

Credit Union #7
Clarkston-Brandon Community Credit Union | $20mm loss

$20mm loss resulting in conservatorship and subsequent merger of the $66mm credit union. The fraud was perpetrated over the course of a dozen years by the CFO. The CFO reportedly created fraudulent documents purporting to show investments held by the credit union. He transferred large sums of money to his personal accounts at various financial service providers. The scheme was finally caught during a routine examination by the state regulatory authority.

Control weaknesses

- **Segregation of Duties:** The CFO had control over all accounting and accounts payable functions. Because he was trusted, no one within the credit union questioned the documents he created.
  The CFO exploited a flaw in the credit union's ACH processing procedure. The lack of segregation of duties over processing of the daily ACH files allowed funds to be transferred from the credit union to his own accounts at various financial service providers.

Credit Union #8
$75mm Credit Union | $240,000 loss

Fraud occurred over a period of two years. CEO was purchasing a lot of computer and related equipment through Amazon using the corporate credit card, for which he approved payment. At the same time, the credit union was going through a core processor conversion. When asked by the supervisory committee why the purchases were so extensive, he justified it by referring to the conversion. Most of this equipment never made it to the credit union. It consisted of printers, scanners, laptops, desktops, etc. Most of it wasn't even shipped to the credit union address. He was selling the equipment the credit union paid for. The fraud was discovered when auditors performed an inventory check of new purchases, and much of it could not be found on premises. The CEO recently plead guilty to this embezzlement.

Control weaknesses

- **Segregation of Duties:** CEO made the purchases and approved the credit card bills for payment. While the accounting manager paid the bill, he did not question when the volume of purchases increased.
- **Lack of Knowledge:** Both the accounting manager and the supervisory committee should have known to look deeper into these purchases. The volume of them did not make sense based on the size and needs of the credit union.

Credit Union #9

$95mm Credit Union | $120,000 loss

Fraud occurred when a long-time employee, who was the vault teller at one of the branches, was made aware of the fact that a member passed away. The husband, who was the survivor, did not understand the financial working of their family, as his wife handled those responsibilities. The employee changed the account to "no-mail" status, and began taking money, mainly in cash withdrawals, at one point from the vault. Over a few months she took about $120,000. The fraud was discovered because as part of the audit and member account confirmation, the auditors reviewed accounts flagged as "no-mail" and selected a large withdrawal for review. As there was no documentation to support this transaction and it was a cash withdrawal from the vault, an investigation ensued.

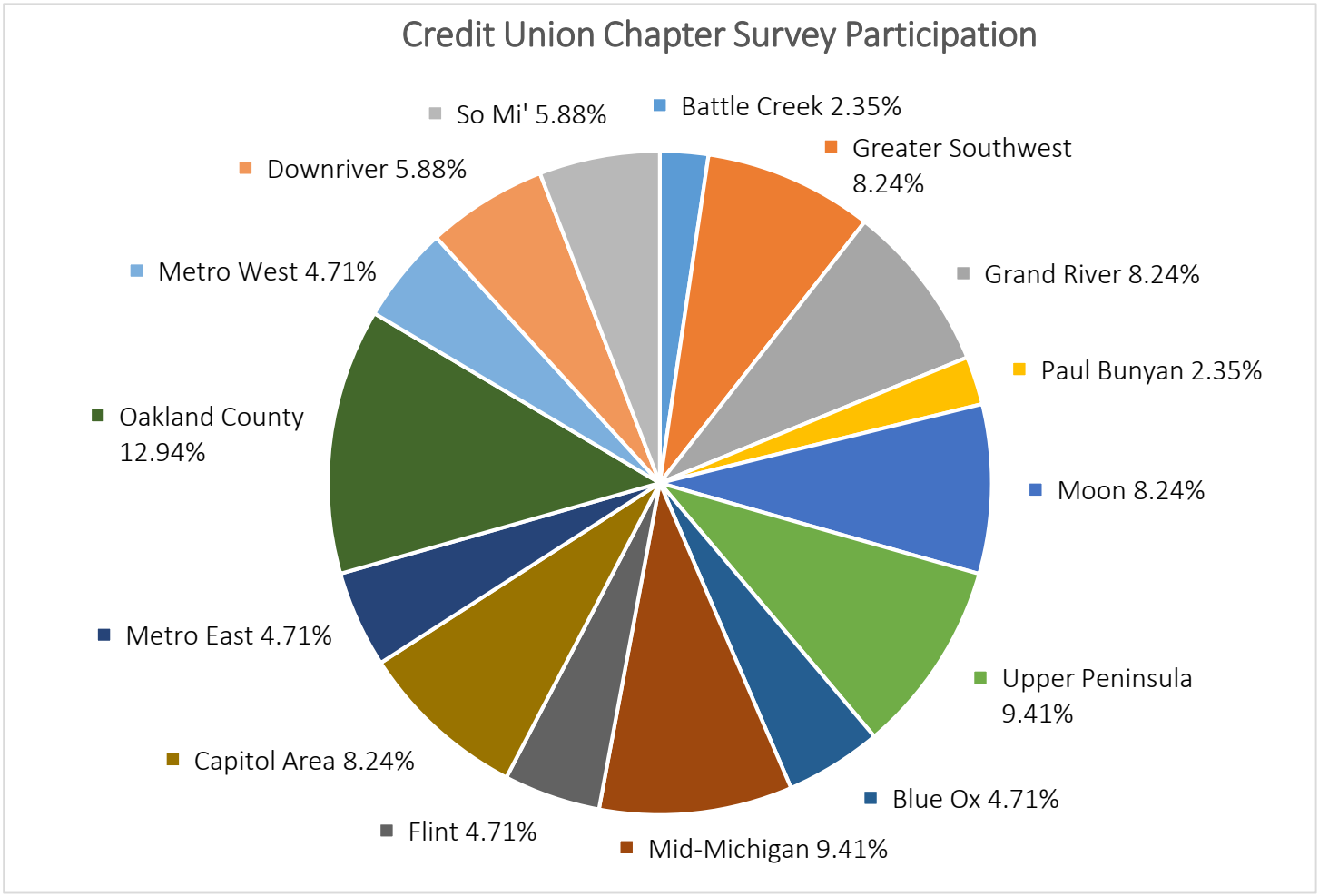
Control weaknesses

- **Segregation of Duties:** Employees with cash access should not have the ability to code member accounts as no-mail. This maintenance should be performed with support from the member, by another individual.
- **Lack of Review:** While the credit union had procedures in place to review file maintenance and vault activity the employee responsible for this did not do her job. She became careless and did not always review the reports. Her review would have caught both the file maintenance and the cash withdrawal for two reasons. First, there should never be a member cash withdrawal from the vault, and second, the size of the withdrawal triggered the Currency Transaction Report filing requirement.

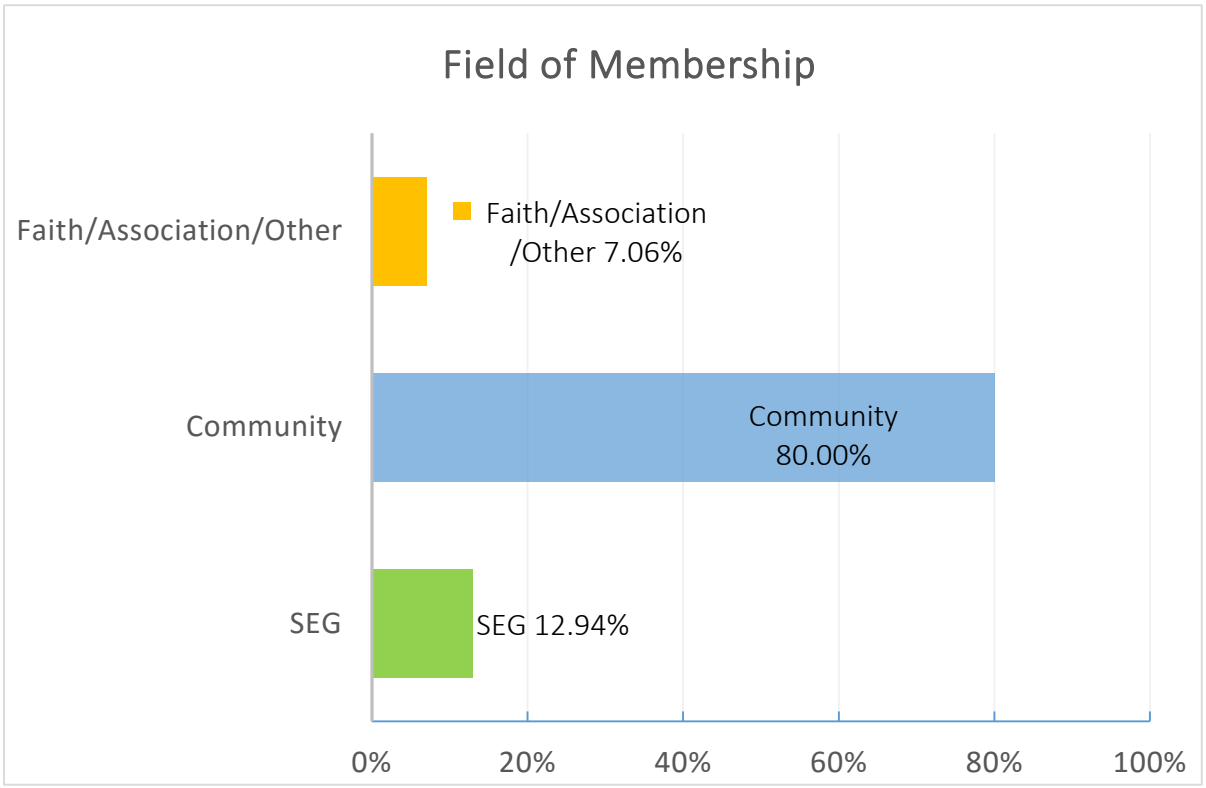
SUMMARY

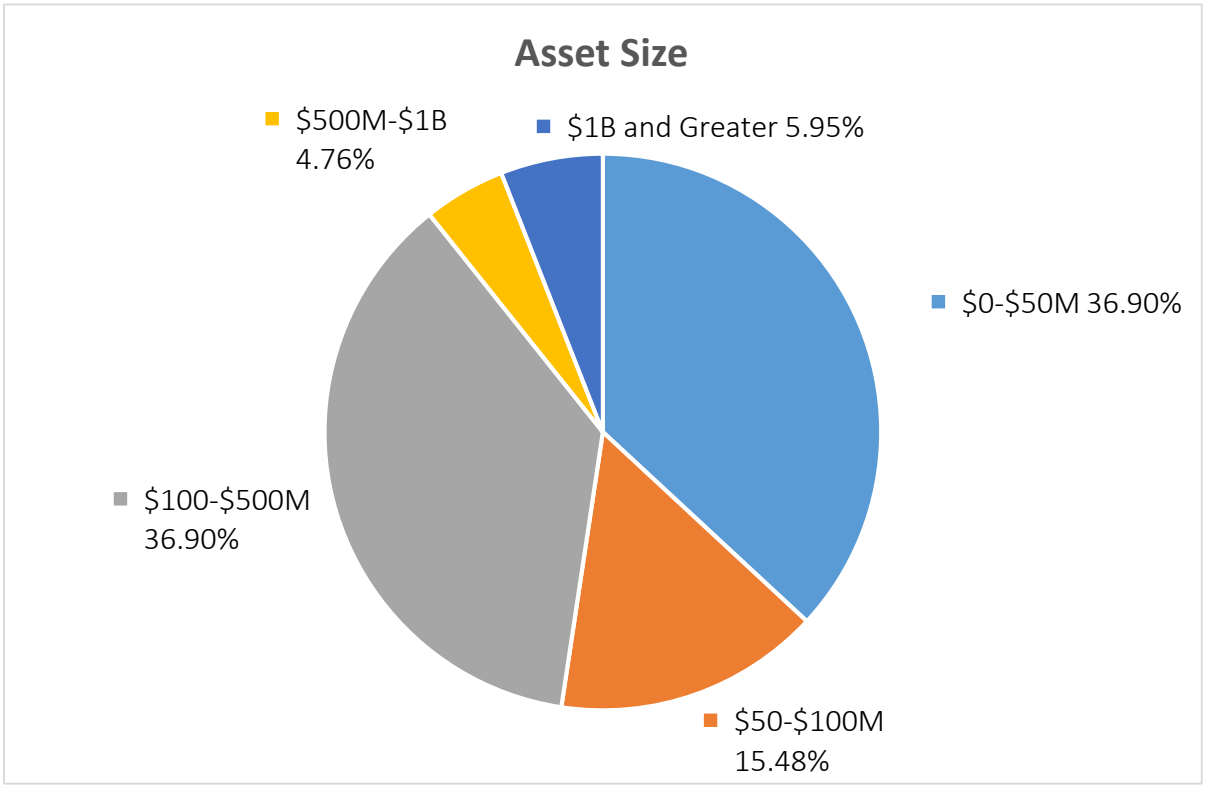
Patterns identified in audits and through case capsules such as these indicate employees can identify a potential fraud due to a lack of segregation of duties. Where weaknesses exist, there should be additional, more detailed reviews.

Appendix B – Internal Controls Credit Union Survey Results

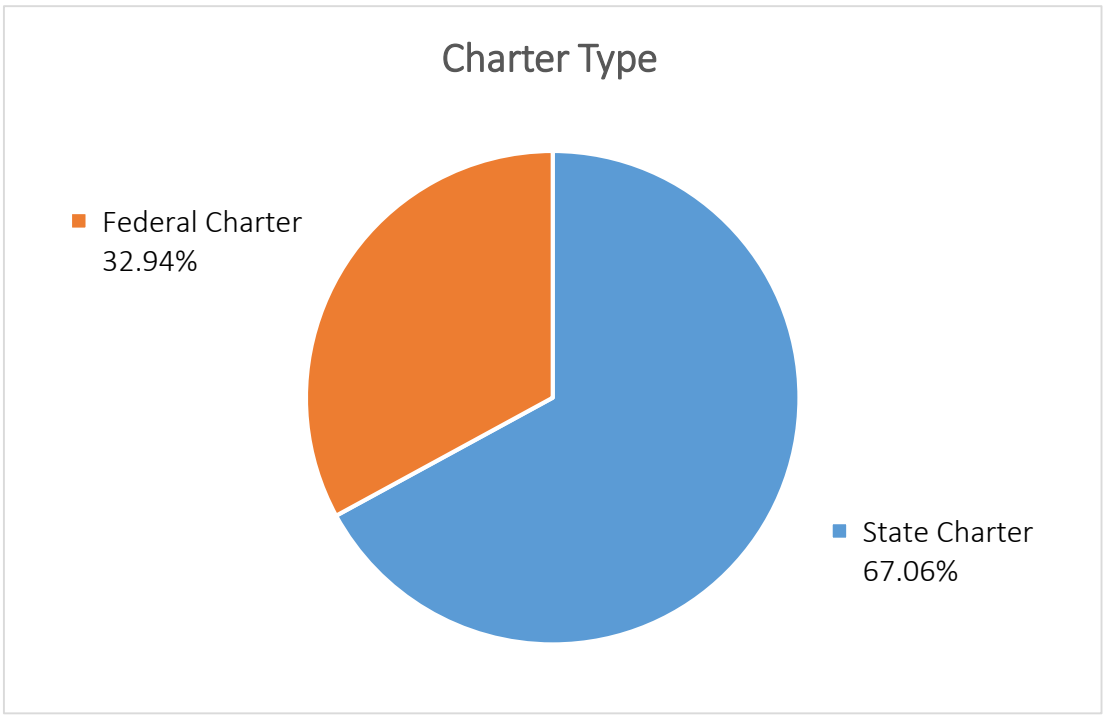


Complete survey results can be found at http://www.mcul.org/regulatory-outreach

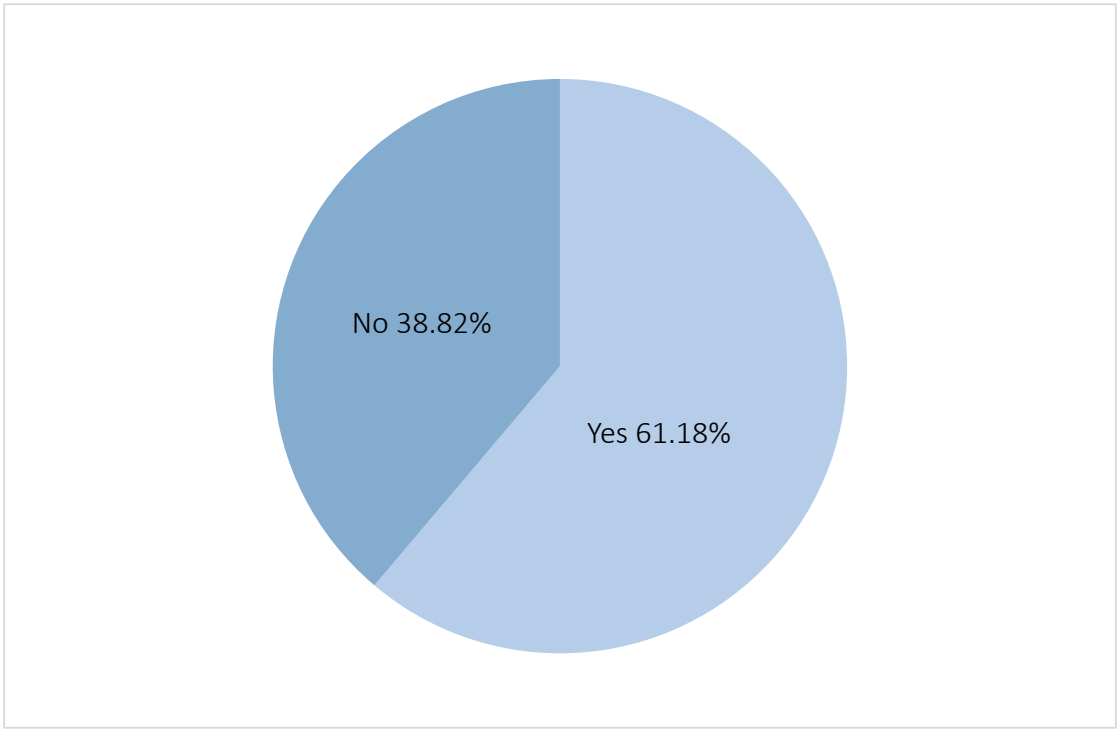




Complete survey results can be found at http://www.mcul.org/regulatory-outreach

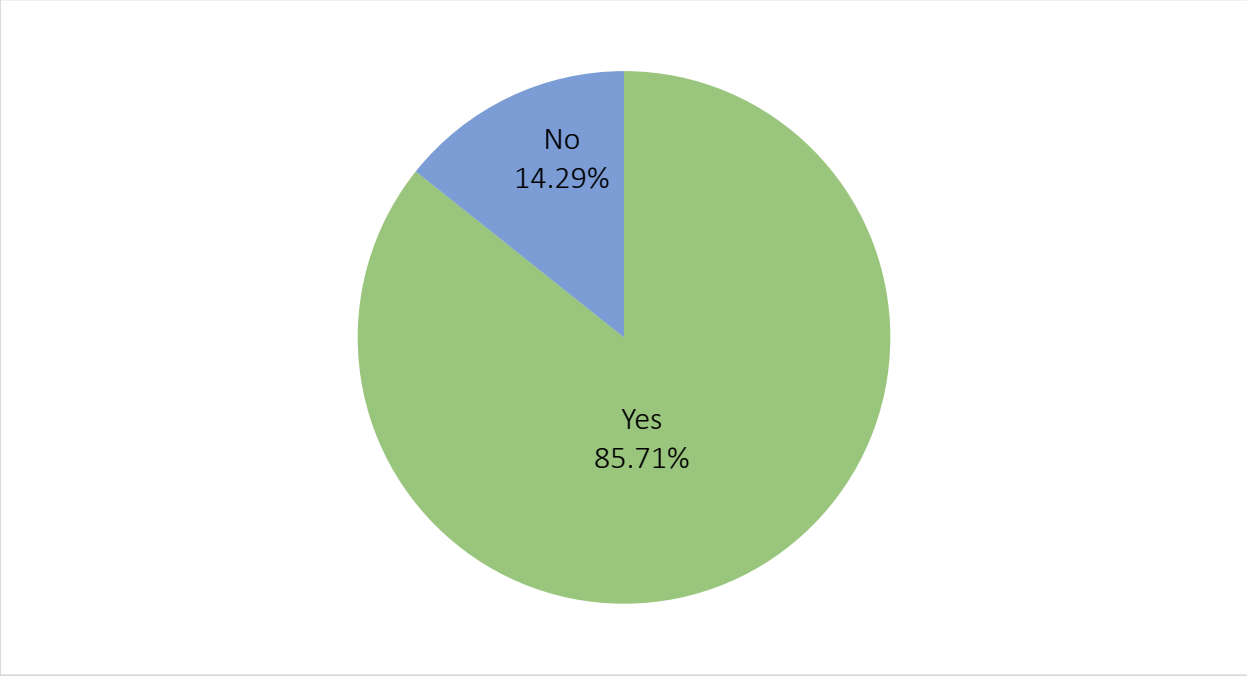


Do you periodically have an internal control audit from a third party to test your internal control environment?



Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Does your credit union have a Supervisory Committee?

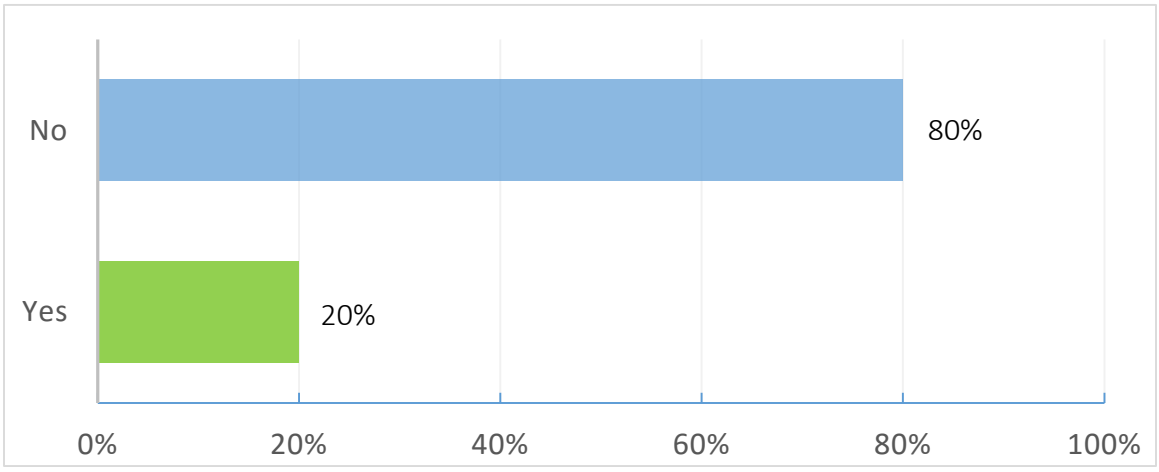


The survey asked respondents, who answered "yes" to this question to provide the scope and frequency of reviews conducted as well as the level of experience of the committee members. Responses included the following:

- "Monthly reviews, annual audit"
- "Quarterly review of external audits and recommends follow up action. Committee consists of one CPA, one corporate audit head and one business leader."
- "The Supervisory Committee reviews check registers, reviews member transactions and does teller balancing on a random basis."
- "Periodic surprise cash counts on teller, vault and ATM. Review CEO and VP level personal account audits monthly."
- "Monthly –teller cash surprise audit, dormant accounts, staff/board personal account review, new loan/closed loan review, delinquent account review, corporate credit card review, new share/closed share review and status of any open audit findings."

Complete survey results can be found at http://www.mcul.org/regulatory-outreach

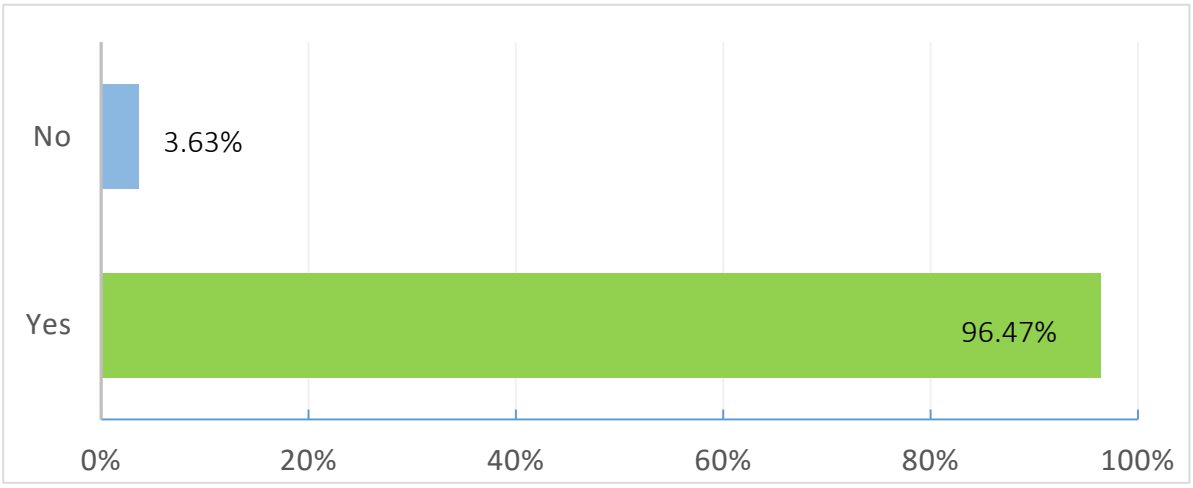
Does your credit union have an Audit Committee?



The survey asked respondents, who answered "yes" to this question, to provide the scope and frequency of reviews conducted as well as the level of experience of the committee members. Responses included the following:

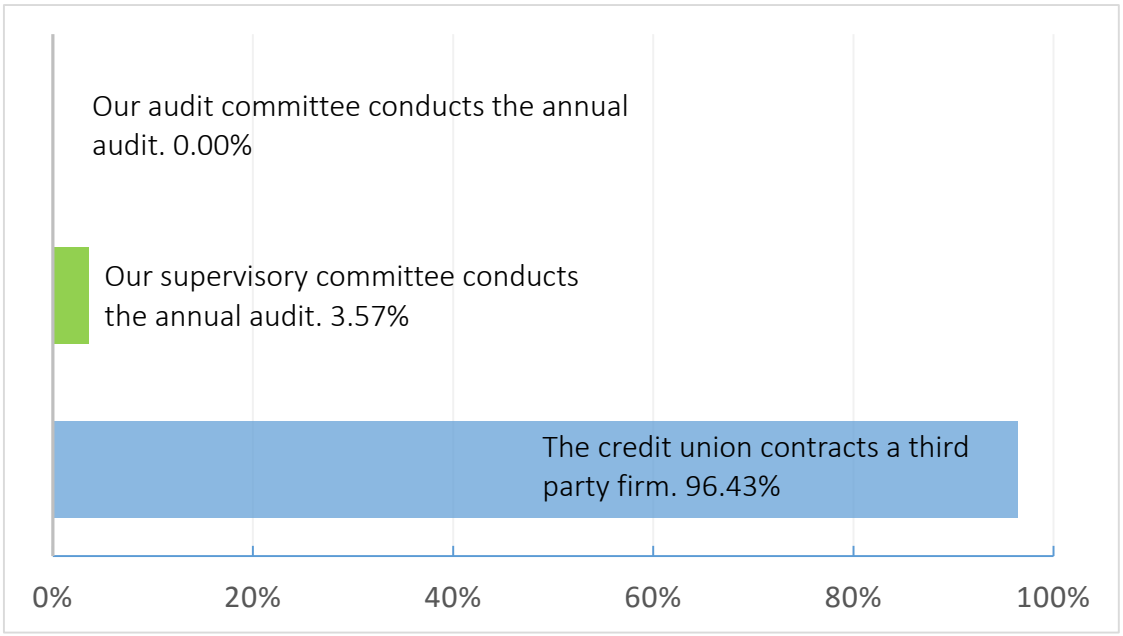
- "They oversee all audits and meet quarterly"
- "Monthly, quarterly and annually. The committee consists of the CEO, operations manager, and directors from the Board with varying years of experience."
- "They are presented all of the audits on a monthly basis to review and approve. The internal auditor gathers the information and presents it to the committee. They are Board members with varying levels of experience."
-

Does your credit union contract for a third party annual audit?

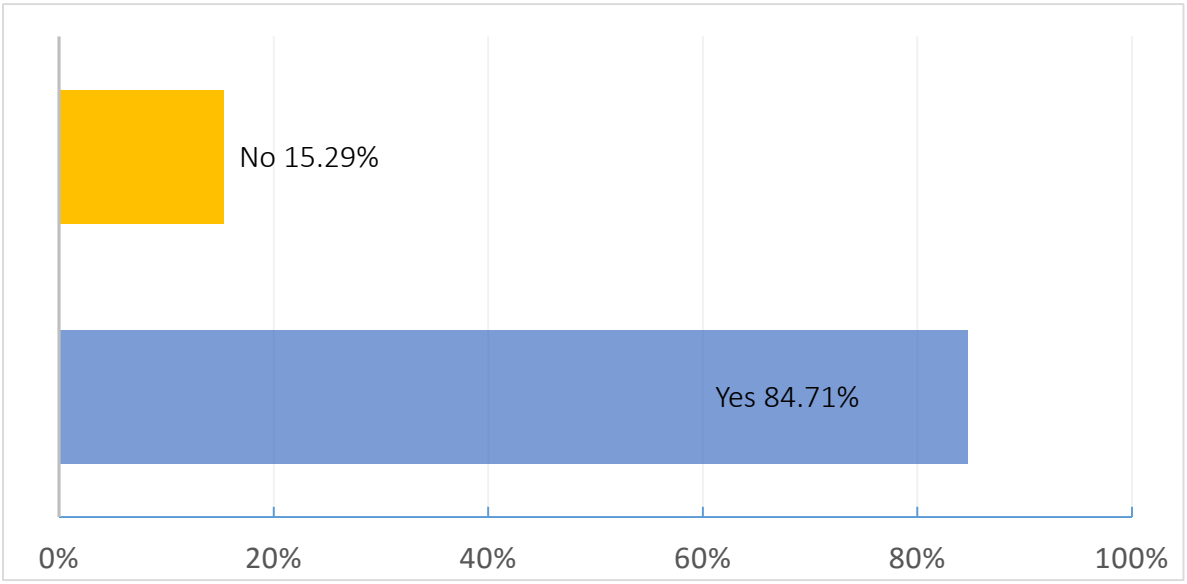


Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Does your credit union conduct an external audit even if not required by Federal or State statute?



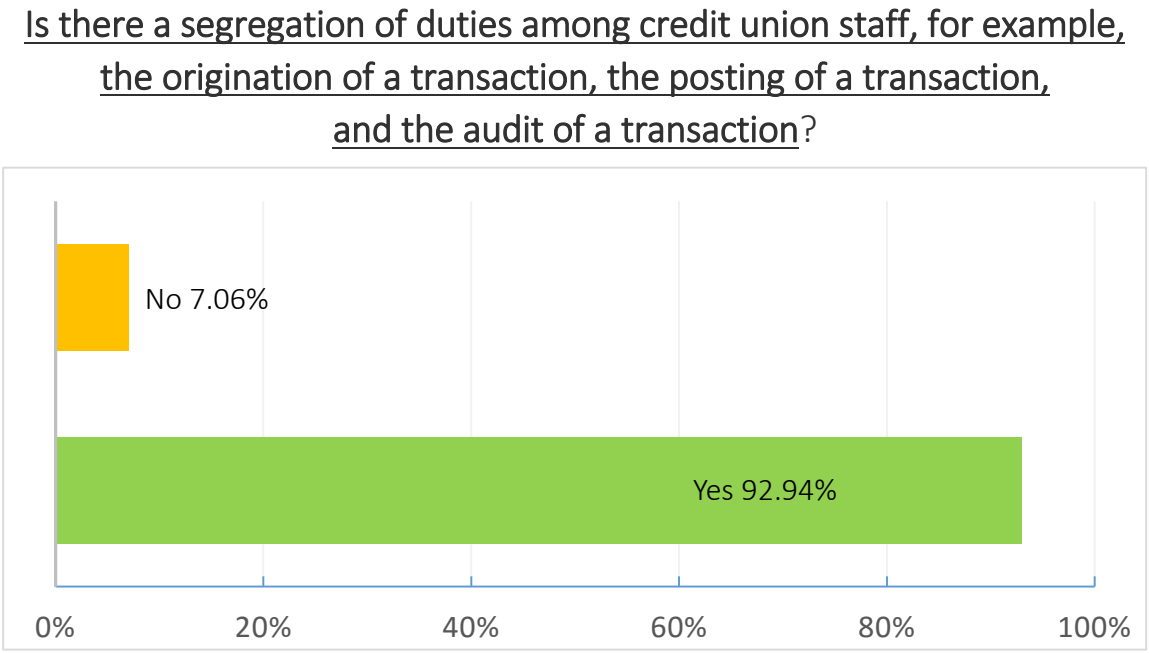
Does your credit union provide for cross-training of staff and a rotation of duties?



Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Respondents provided comments addressing cross-training and rotation of duties. Comments reflect the following:

- "Require five consecutive days off and job functions be performed while they are out."
- "Critical or high-risk functions identified by the credit union have a primary and back-up that performs the role."
- "All departments have cross-training to ensure that all responsibilities are covered when other employees are not available."
- "Rotation is done only when needed, such as vacations, etc."
- "Since we have limited staff the cross-training is limited just enough to cover for vacations."

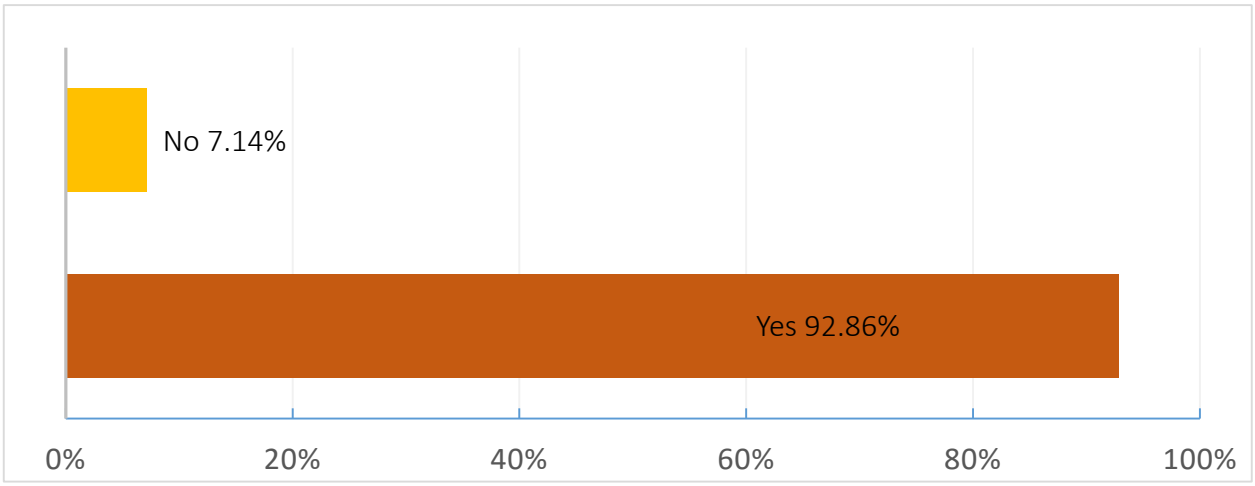


Respondents provided comments addressing segregation of duties among credit union staff. Comments reflect the following:

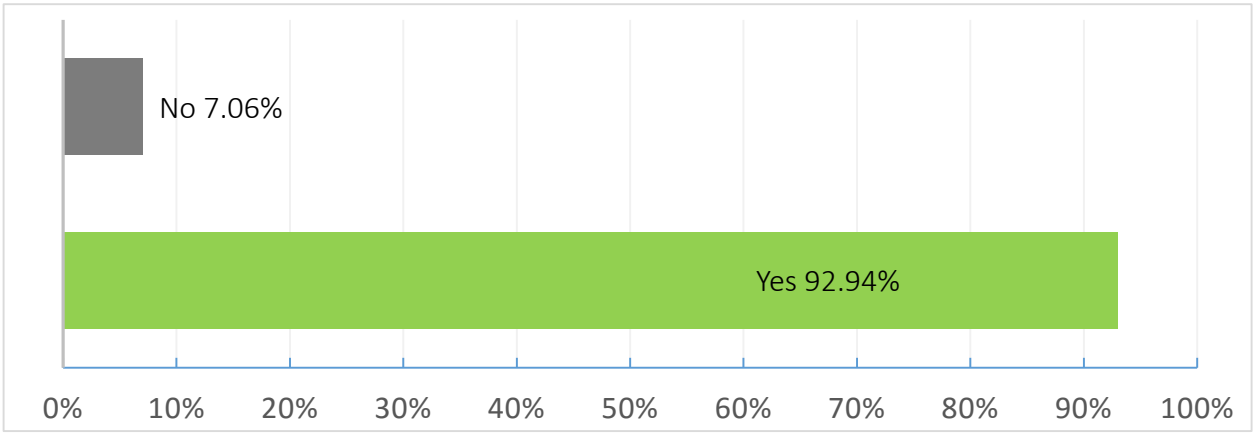
- "Our core processing system permissions enforce segregation of duties addressed."
- "Separation of duties exists for process that handle cash, wires, ACH, corporate checks, loan funding, etc."
- "Loan originators cannot approve loans. Individuals taking member wire requests cannot send the wires. Most executives are 'view only' on many systems. For those who are not, all transactions are reviewed by the CEO."
- "We have a loan review process performed by our risk management department to ensure proper controls and that loans are approved within our underwriting policy guidelines. Segregation of duties are in place for all key processes."
- "A loan officer cannot approve a loan and fund a loan. If necessity dictates that they had to (due to limited staff), then that loan is automatically selected for audit. Mortgage loan officers do not process their own file. Vault cash and keys are under dual control. Internal audit verifies cash periodically. All teller drawers are audited at least monthly and prior to any extended vacations."

Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Are Vaults, ATMs, Cash Dispensers and Alarm Systems managed under dual control?



Are surprise cash counts conducted periodically by auditors or the supervisory committee?

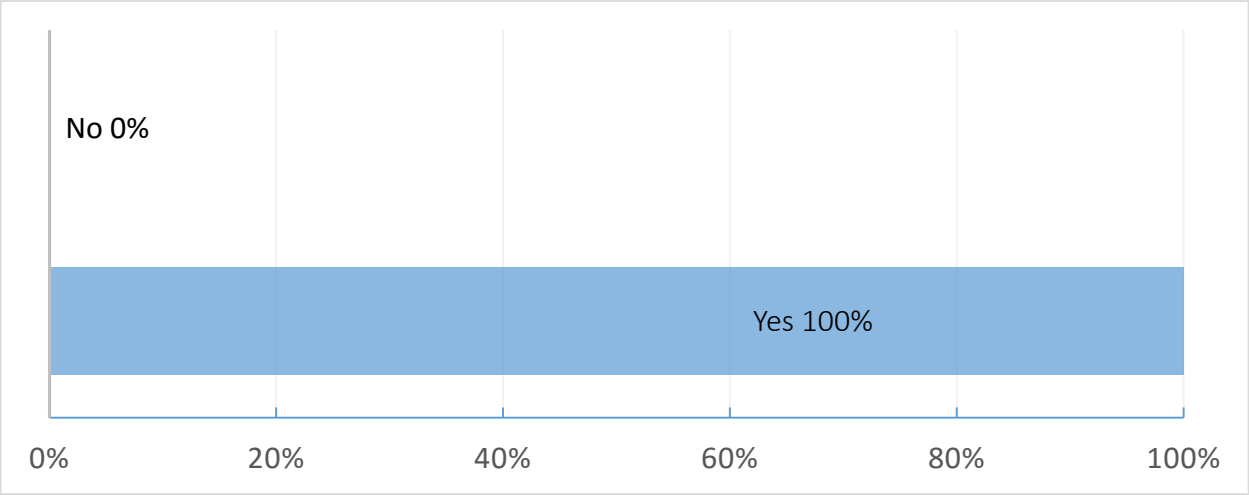


Respondents provided comments regarding frequency of surprise cash counts as follows:

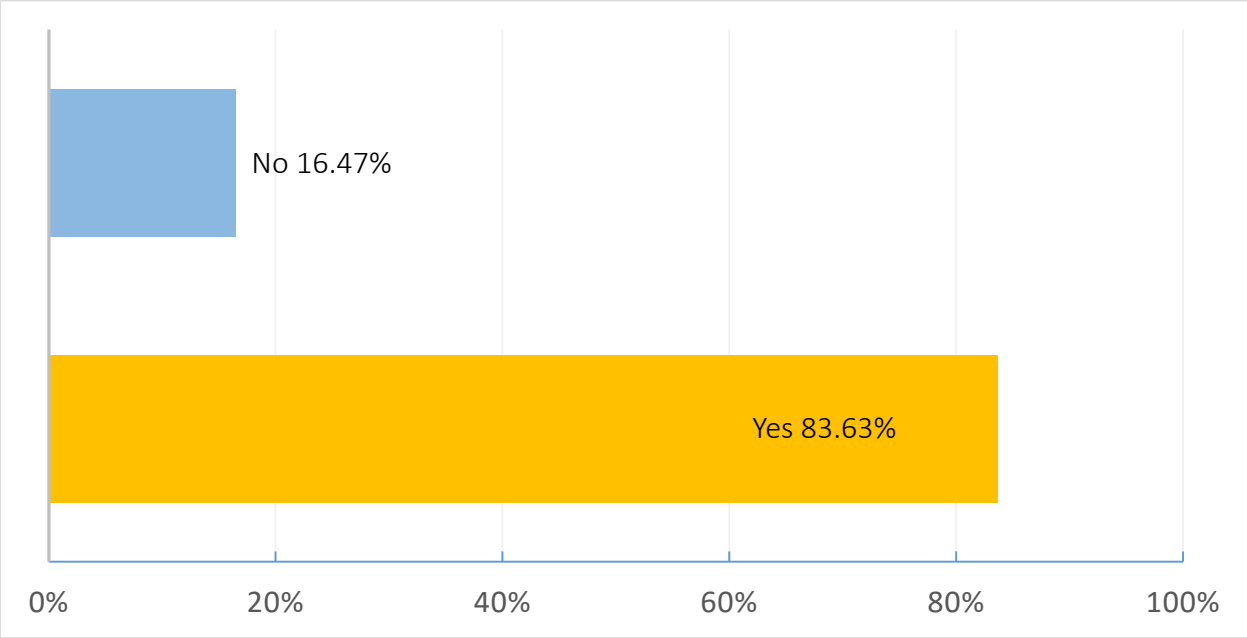
- "Conducted monthly by the accounting supervisor and quarterly by the supervisory committee."
- "Conducted monthly and quarterly by internal staff under dual control. Three times a year by external audit. We also conduct random audits, vacation audits and vault ownership changes and audits."
- "Supervisory Committee quarterly; auditor annually, counts by management when staff go on vacation."
- "Internal Audit conducts. The frequency is based on a location's risk profile as determined by an Internal Audit."

Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Are records of teller overages and shortages maintained by management?

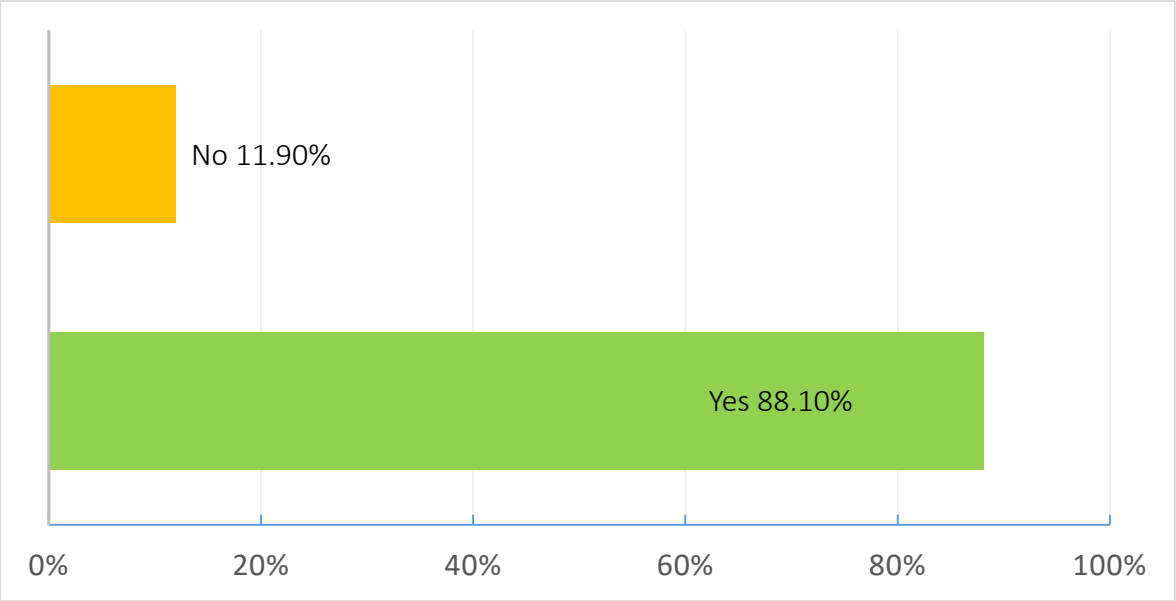


Are system parameters updated to reflect changes to accounts of family members and significant others?

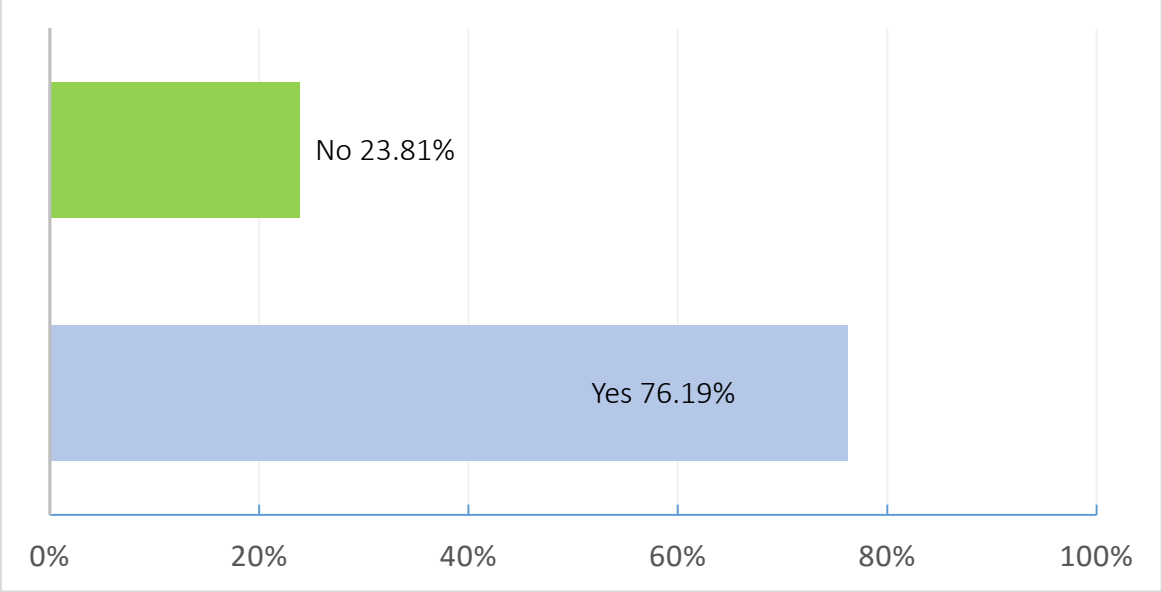


Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Is an independent review of transactions made to accounts of employees, their family members or individuals living at the same address periodically conducted?

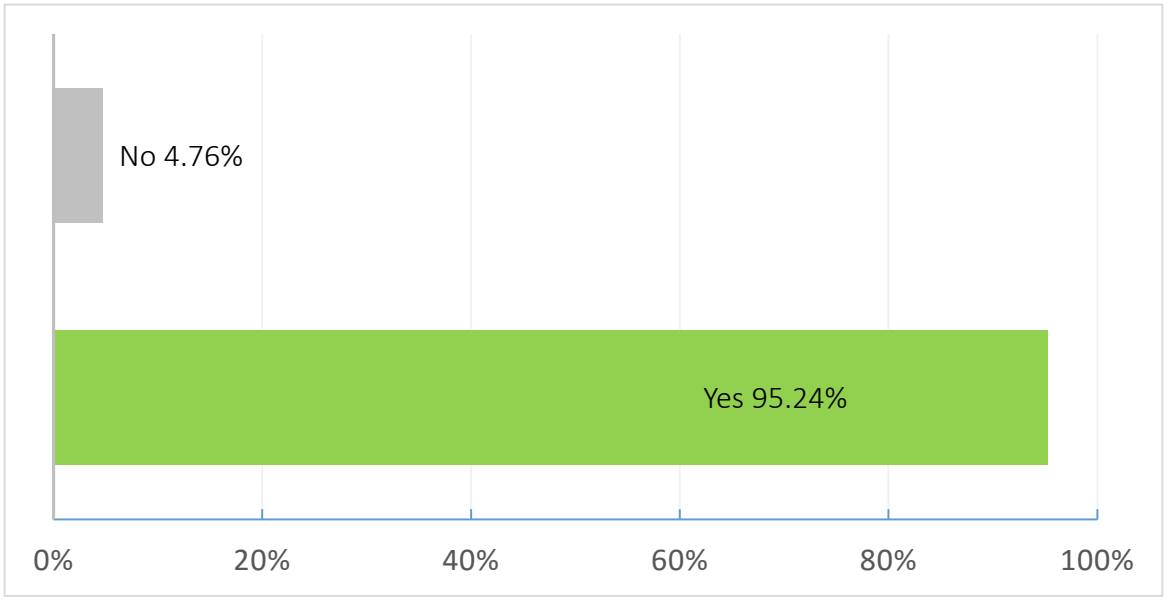


Is there a segregation of duties among staff who can open new accounts vs. approve new loans?

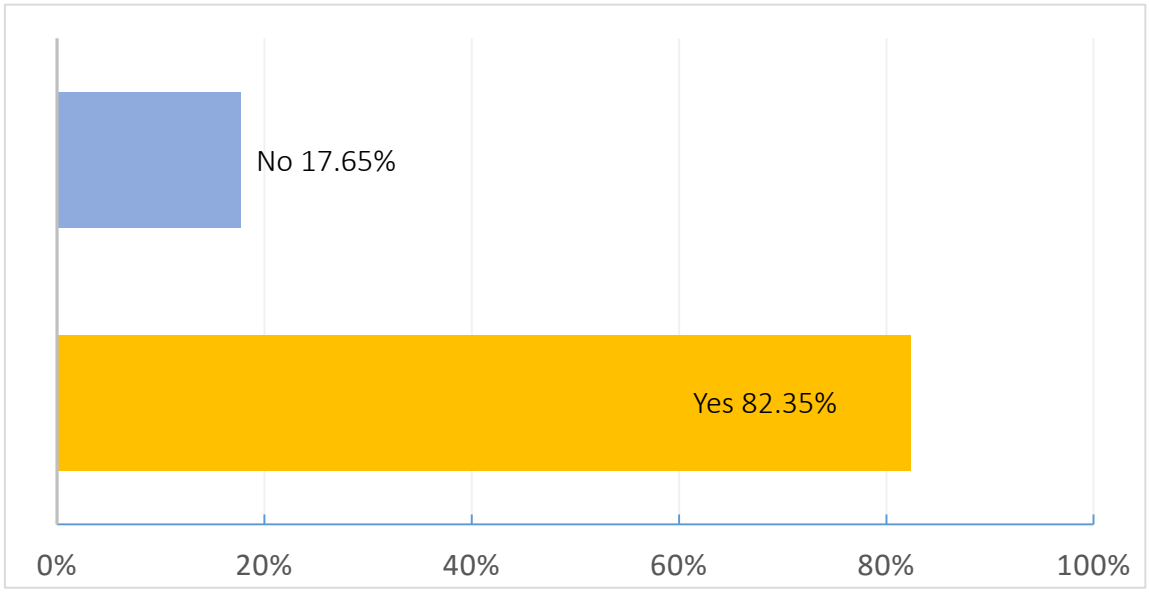


Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Are supervisory overrides in place to restrict specific employee transactions?

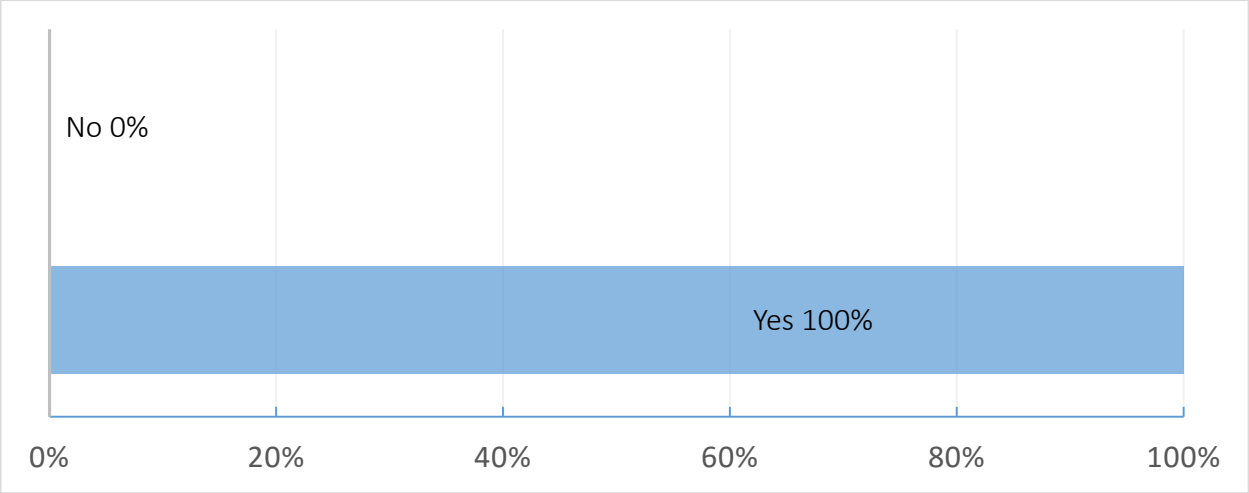


Are override reports generated and reviewed regularly by management, internal audit, audit committee or supervisory committee members to assure all override transactions were authorized?



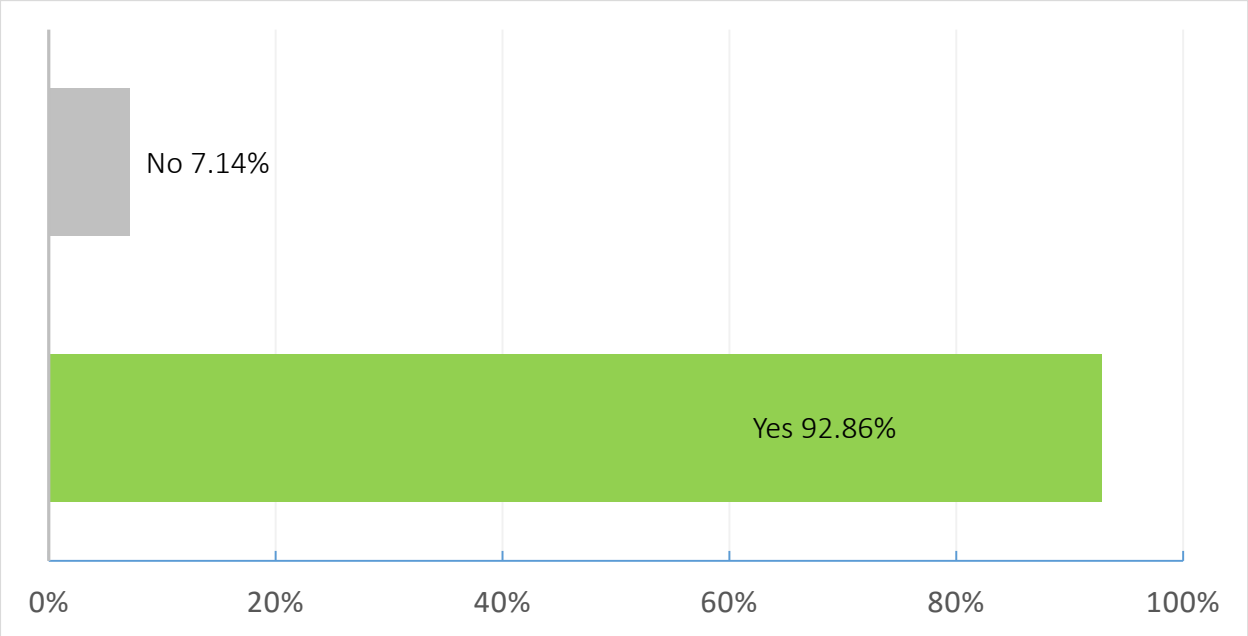
Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Are accounts flagged for dormancy/inactivity after 12 months or in accordance with the credit union's policy and are such accounts monitored for activity?



Are file maintenance reports monitored and reviewed by management, internal audit, audit committee or the supervisory committee regularly?

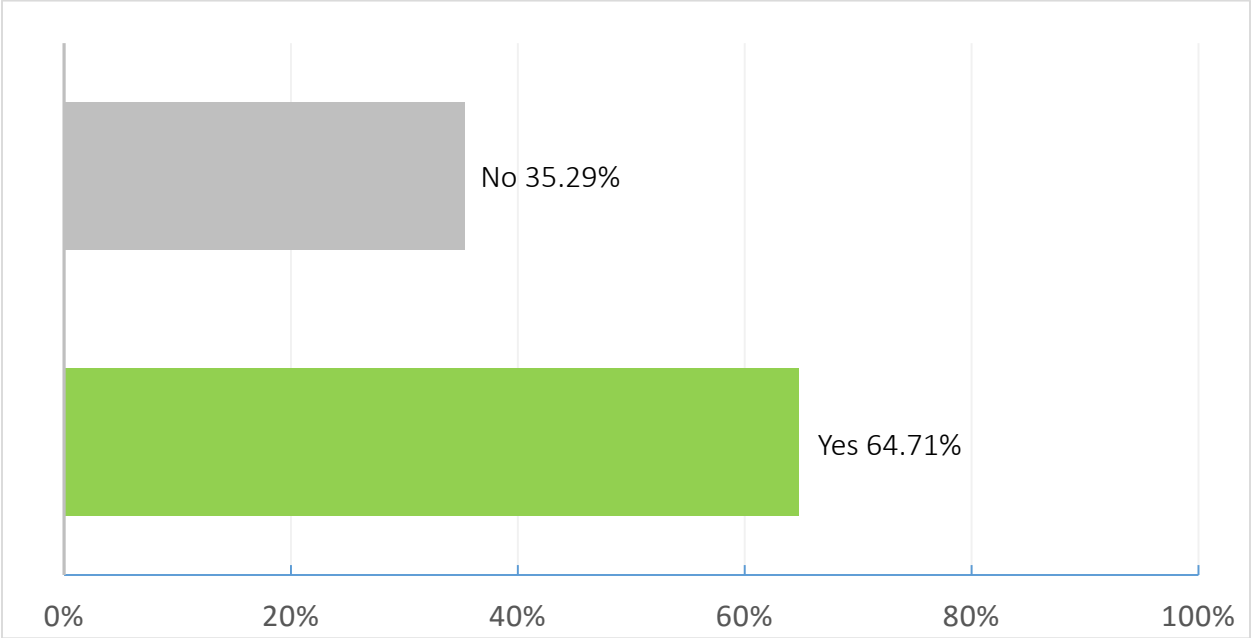
The type of file maintenance that should be reviewed include data changes at an account or member level.



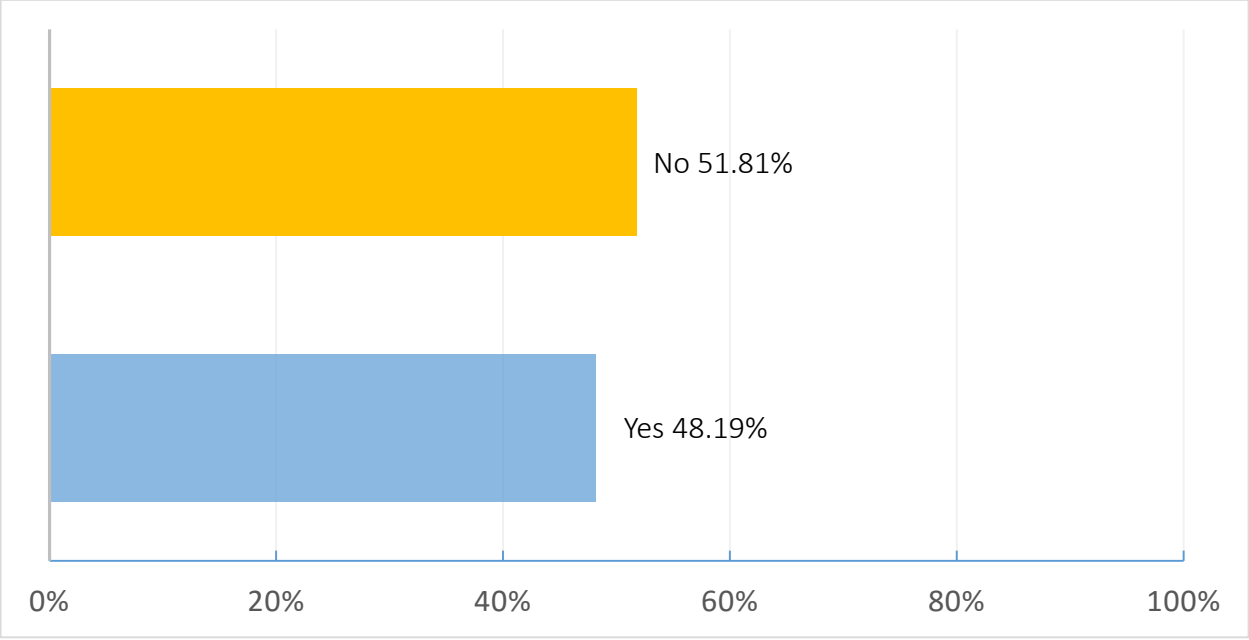
Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Does the credit union separate loan approval and disbursement duties?

An increase in fictitious/unauthorized loans can result when loan approval and disbursement are handled by the same employee.



Does credit union collection staff have loan approval authority or file maintenance authority?

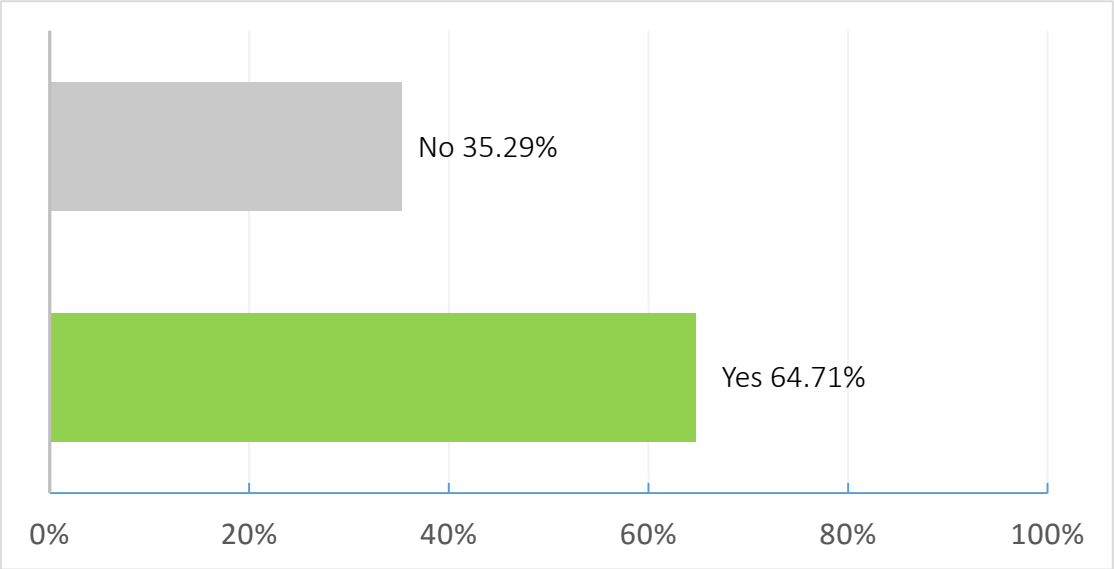


Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Respondents provided comments as to the approval and file maintenance authority for collection staff as follows:

- "Group can perform loan modifications. Final approval is restricted to the manager. Dual control through the COO."
- Employees responsible for collections are able to perform loan modifications or extensions. However, dual controls exist governing the approval and disbursal during this process. These employees can also make file maintenance changes, however, file maintenance reports are reviewed by Internal Audit on a daily basis."
- "Collection Manager can modify rate and terms related to modifications and TDRs. A report is reviewed weekly for any file maintenance changes."
- "The Collection Department is able to approve work out loans with the correct approvals from management."

Is there a segregation of duties and rotation among staff handling credit union investments and are these transactions handled under dual control?

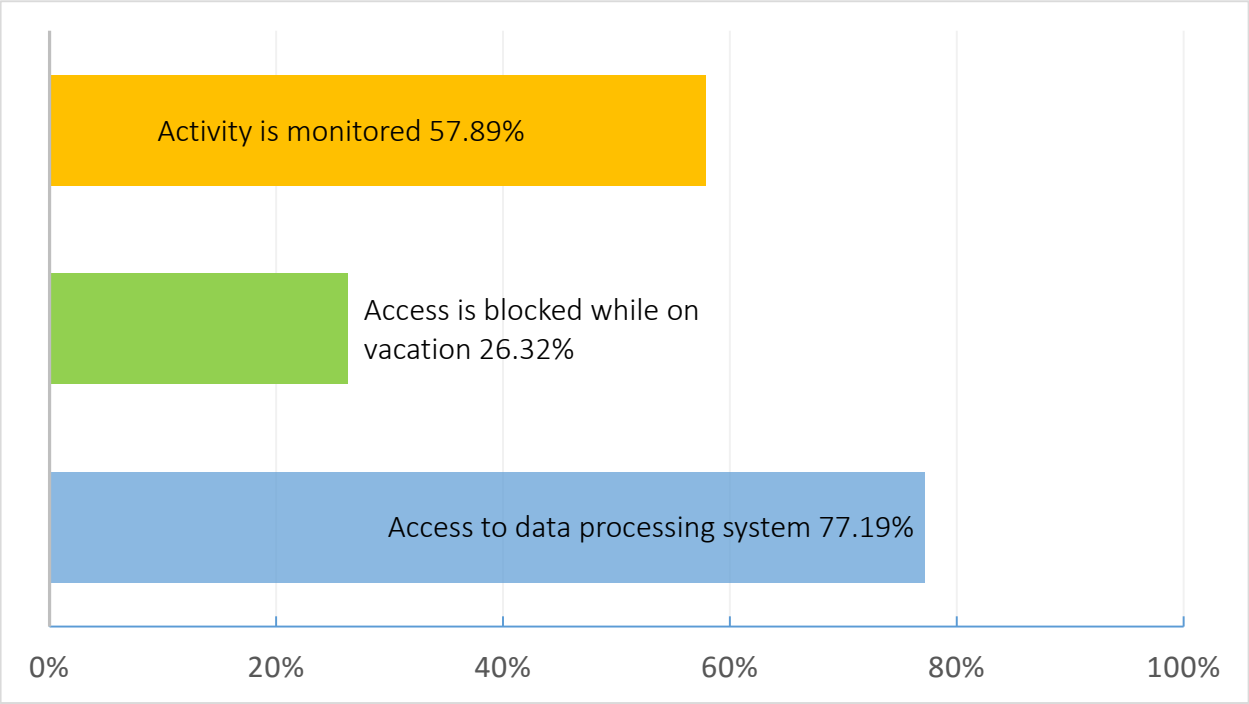


Comments addressing segregation of duties among staff handling investments included:

- "The CEO makes the investment decisions, the VP of lending books the investments, and the VP of compliance wires the funds for the investments."
- "Investments are approved by the CEO however transfer of funds must be completed by a second person."
- "Our CEO creates the investment, the accounting manager or supervisor will verify and wire funds, another accounting clerk does the balancing, and it is also checked by the audit/compliance department."

Complete survey results can be found at http://www.mcul.org/regulatory-outreach

If credit union management and staff are permitted remote access what is their level of access and are controls in place? *(please select all that apply)*



Respondents further discussed the restrictions imposed as follows:

- "Limited to those with need to have that access. Remote access activity is reported weekly and reviewed by CEO and IT Support team member. Remote access is blocked for a minimum of one week when an individual(s) is on vacation."
- "There is no remote access permitted."
- "We only have email remote access. No financial access."
- "Leadership teams are removed from access to critical data processing and other critical software during their vacation."
- "Only a couple of senior managers have access remotely and can only view shared folders and NOT the data processing system."

Complete survey results can be found at http://www.mcul.org/regulatory-outreach

Appendix C – Introduction and Sample Risk Assessment

This risk assessment tool is intended to be generic in nature and ideally be a template or guide for credit unions. To truly assess the risk for fraud within a credit union, each credit union needs to assess the inherent risk of each respective area of operations for the susceptibility for fraud. Additionally, credit unions will need to evaluate the internal controls that are currently in place over each area to ultimately determine the true fraud risk.

Internal Fraud Risk Assessment										
			Inherent Risk				Mitigated Risk			
Functional Area	**Process/Procedure**	**Fraud Possibility**	**Likelihood (1-5 = Low-High)**	**Impact (1-5 = Low-High)**	**Overall Risk Rating (1-10 = Low-High)**	**Action to Mitigate Risk**	**Likelihood (1-5 = Low-High)**	**Impact (1-5 = Low-High)**	**Overall Risk Rating (1-10 = Low-High)**	**Residual risk**
Deposit Operations (new/closed/dormant, IRA, overdraft)	New Account Opening	Creation of fake accounts that can be used to open loans which are used to embezzle funds				Have a second person confirm the identifying documentation used to open the account. Restrict the ability of those with new member account opening responsibilities from approving and disbursing loans.				
Deposit Operations (new/closed/dormant, IRA, overdraft)	Returned Mail/Bad Address	Active/Dormant accounts can be accessed without member knowledge; returned plastic cards can be activated				Mailings sent to members at old and new address to verify address. Create special codes for accounts with bad address and create file maintenance and transaction logs for these specific codes to identify transactions that are generated by credit union employees.				
Branch Operations	Change Fund Differences	Theft				Dual control for cash counts, supervisor overrides for teller over/short, reconciliation of vault GL by independent party, surprise vault and drawer audits, regular branch manager audits, regular ATM audits completed at unpredictable intervals. Review GL history for transfers or credits from the change fund general ledgers to other non-change fund general ledger accounts				
Branch Operations	Manipulation of Transactions	No receipt provided to the member for proof of the transaction. Vault cash sales can be inaccurately stated				Surprise cash counts, branch security (ex: cameras), balancing policies (ex: over and short), regular (and surprise) vault teller audits				

Internal Fraud Risk Assessment										
			Inherent Risk				Mitigated Risk			
Functional Area	**Process/Procedure**	**Fraud Possibility**	**Likelihood (1-5 = Low-High)**	**Impact (1-5 = Low-High)**	**Overall Risk Rating (1-10 = Low-High)**	**Action to Mitigate Risk**	**Likelihood (1-5 = Low-High)**	**Impact (1-5 = Low-High)**	**Overall Risk Rating (1-10 = Low-High)**	**Residual risk**
Collections/ORE/Loan Modifications)	Account/Loan File Maintenance	Advancing due dates on employee accounts, changing addresses, changing statuses to suppress mailing				Supervisor overrides required for account/loan file maintenance. Reports of activity are kept for review of account activity				
Deposit Operations (new/closed/dormant, IRA, overdraft)	Dormant Accounts	Accessing funds, "activating" account which stops monitoring as "dormant"				Supervisor overrides required for transactions on dormant accounts. Reports of activity are kept for review of account activity by a second department. Reviewing of file maintenance logs for accounts that have moved from dormant to active. Testing a sample of those transactions by comparing signature cards and transaction receipts to validate the member completed the transaction.				
Printing Checks		Print checks from member accounts, print checks from fictitious accounts				Difficult to monitor as members request counter checks. Structure a centralized member complaint system so that member concerns are monitored and documented. Keep check stock locked and under dual control. Using IT systems, restrict access to check issuing to those with a logical need for the access.				
Plastic Card Operations (Debit/ATM/Credit)	Issuing new ATM/Debit/Credit Cards	Creating fictitious cards, funding pre-paid cards from member accounts.				Dual control to create cards (debit). VISA cards ordered by separate department (other than lending) Pre- paid cards log maintained. Segregation of duties between account opening and new card activation. Require secondary approval for a new debit card.				

Appendix D – Anti-Fraud Certification

(Insert date)

(Insert Credit Union Name)

Voluntary Anti-Fraud Control Certification

The Board and CEO of _____(Credit Union Name)_____ certify the following:

- The Anti-Fraud and Internal Controls white paper has been distributed to the Board and Senior Management, who have reviewed its contents.
- The credit union has reviewed its anti-fraud policies and procedures and internal controls and evaluated whether different or additional controls are required.
- The credit union has evaluated whether periodically, if an expanded scope external audit by an independent party is appropriate.
- An anonymous, toll-free fraud prevention hotline will be circulated to staff and volunteers to encourage reporting of suspicious behaviors.

(Insert signature blocks)

_____

(Insert Printed Name)

(Insert Title)

(Insert Credit Union Name)

_____

(Insert Printed Name)

(Insert Title)

(Insert Credit Union Name)

Appendix E – Model Policy

SAMPLE INTERNAL FRAUD MANAGEMENT POLICY AND PROCEDURE

INTERNAL FRAUD POLICY

I. Purpose of Internal Fraud Policy

The Credit Union's Internal Fraud Policy is established to facilitate the development of controls that will aid in the detection and prevent of fraud against XXXX Credit Union. It is the intent of XXXX Credit Union to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

II. Scope of Internal Fraud Policy

This policy applies to any irregularity, or suspected irregularity, involving directors, committee members, and employees as well as consultants, vendors, contractors, outside agencies doing business with employees of such agencies and/or any other parties with a business relationship with XXXX Credit Union.

III. Definition of Fraud

Fraud can be broadly defined as an intentional act of deceit to obtain an unjust/illegal advantage. For the purposes of the policy, fraud shall include but is not limited to:

Theft or misappropriation of assets owned or managed by XXXX Credit Union;

Submitting false claims for payments or reimbursement;

Accepting or offering a bribe or accepting gifts or other favors under circumstances that might lead to the inference that the gift or favor was intended to influence an employee's decision-making while serving XXXX Credit Union;

Accepting a gift from anyone doing business with XXXX Credit Union except as permitted by XXXX Credit Union's Bank Bribery Act policy.

Blackmail or extortion;

"Off the books" accounting, or making false or fictitious entries or any other impropriety in the handling or reporting of money or financial transactions;

Knowingly creating and/or distributing false or misleading financial reports;

Paying of excessive prices or fees where justification thereof is not documented;

Violation of the Bank's procedures with the aim of personal gain or to the detriment of XXXX Credit Union;

Willful negligence intended to cause damage to the material interest of XXXX Credit Union; and

A dishonorable or reckless or deliberate act against the interests of XXXX Credit Union.

Profiting as a result of insider knowledge concerning anything involving XXXX Credit Union.

IV. Other Irregularities

Irregularities concerning the conduct of any of the persons described in Section II must be addressed by management but if they do not involve fraud they may be handled through normal personnel channels.

Actions that may or may not involve fraud include (but aren't limited to) the following:

Disclosing confidential and proprietary information of XXXX Credit Union to outside parties.

Disclosure of member and other customer information to outside parties except as authorized.

Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment.

If there is any question as to whether an action constitutes fraud, contact XXXX or YYYY for guidance.

V. Responsibility for the Prevention and Detection of Fraud

All directors, committee members, and employees have a duty to guard against fraud. Employees are expected to identify processes and procedures that may be vulnerable to fraud and to draw such instances to the attention of management in their department.

Management has a particular responsibility to be familiar with and alert to the types of fraud that might occur in their area and to put in place effective controls to avoid such occurrences.

Management shall provide support to and work with the [Internal Auditing Department/Outside Auditors], other departments, and law enforcement agencies in the detection, reporting and investigation of dishonest or fraudulent activity, including the prosecution of offenders. Once fraud is detected, heads of departments are responsible for taking appropriate corrective action to ensure adequate controls are put in place to prevent reoccurrence of improper activity. Managers shall be conscious that, given the widespread use of IT systems, and the separation of controls across divisions, fraud may come to light in departments other than those in which they are committed.

INTERNAL FRAUD PROCEDURE

I. Reporting a Suspected Fraud

Reporting fraud according to the following procedure is **mandatory** for any director, committee member, or employee who suspects that a fraud has occurred. Persons who cover up, obstruct, or fail to report (or monitor) a fraud that they become aware of, or ought to have been aware of, may be considered to be an accessory after the fact and may be subject to XXXX Credit Union's disciplinary policies which could involve action up to and including dismissal. Persons who threaten retaliation against a person reporting a suspected fraud shall be subject to the disciplinary policies which could include action up to and including dismissal or prosecution or both.

Great care must be taken in dealing with suspected dishonest or fraudulent activities to avoid:

Alerting suspected individuals to an investigation underway;

Treating employees unfairly; and

Making statements that could lead to claims of false accusations or other charges.

Details of the incident, facts, suspicions or allegations should not be discussed with anyone inside or outside of XXXX Credit Union unless XXXX Credit Union's investigating team specifically directs this or the discussion is requested by a regulator having jurisdiction over the credit union or an appropriate law enforcement agency. In particular, the matter should not be discussed with the individual suspected of fraud.

Fraud can be detected at any level within XXXX Credit Union, and the following will apply in the reporting of suspected internal fraud:

An employee or other person who suspects that fraudulent activity is taking place should, in the first instance, report the matter to the manager of the employee's department or, if the person is not an employee, to the manager of the department involved.;

If an employee does not feel comfortable raising a matter with the department manager – due to the nature of the concern, its seriousness, or for some other reason – the employee may raise it immediately with [indicate alternative contact point, such as the credit union's outside auditor or anonymous hotline].

In certain cases, it may be more appropriate to raise the matter with someone more senior (e.g., a member of the Operations/Audit Committee), perhaps because of the seriousness or sensitivity of the matters concerned. If an employee wishes to speak to [name of highest administrative position] or higher grade in confidence, the employee should raise this with [name of contact point] at the outset so that appropriate arrangements may be made in this regard.

Concerns may be reported verbally or in writing. Where a concern is raised verbally the following steps are to be taken by the employee raising the concern to ensure that the concern raised is acknowledged by the recipient as received in the manner intended by the employee. These steps are to ensure that the recipient is clear that what is intended as a concern about suspected fraud is not construed by the recipient as a passing or casual comment.

1. The employee raising the concern sends a written communication to the recipient.

   The written communication confirms:

   a. The fact that a concern about suspected fraud was raised (details of the suspected fraud need not be included, just the fact that a concern is raised)

   b. That a written acknowledgement from the recipient to the employee is required.

2. The recipient responds with a written communication acknowledging receipt of the concern.

Once a report of suspected fraud is made to a supervisor/manager, that person is required to pass that information promptly to [person in next step in the process];

The [person in charge of next step of process] on receipt of a report of a suspected fraud is required, in turn, to report the matter promptly to [party responsible for investigating fraud].

The person reporting the fraud should be instructed not to discuss the situation with anyone except with the approval of [person who gives approval].

To encourage employees to report fraud, XXXX Credit Union shall insure that all employees are aware of Whistleblower's protections available under federal and state law.

In some cases, suspected fraud may be reported anonymously. The credit union has established a hotline for this purpose at xxx-xxx-xxxx. If this occurs, the party receiving the report must report the suspected fraud to [department that investigates fraud allegations, or the Board Chair or Supervisory Committee Chair] which, in turn, shall take the required steps to investigate. Information concerning the hotline shall be made available to all directors, committee members, and employees. Employees making a report in this manner should record the time and details of their report so if they are later accused of failing to report something they were obligated to report; they can use the hotline report as evidence of meeting the reporting requirement. The operator of the hotline may establish a confirmation number process for this purpose.

II. Procedure for the Investigation of Alleged Fraud

No investigation of a suspected fraud should take place until the [name of appropriate position] has been informed. That person, in turn, will determine who best to inform [internal audit committee, outside auditor, etc.]. The [department responsible for investigating frauds] must investigate all instances of suspected frauds reported to them.

The manager of [the department that investigates fraud] (except in any case involving his or her department) will take the lead when fraud investigations are being conducted. This will involve data collection, analysis and intervention, including the review of internal controls. In circumstances where the investigation requires the use of technical expertise, which Internal Audit may not possess, external specialists (subject to the approval [approval authority]) may be appointed to lead (if the case involves the department responsible for investigating frauds]) or to contribute to the investigation.

The manager of [the department that investigates fraud] will conduct an initial investigation to gather factual information and reach a preliminary view as to whether further action is required. This manager will report the findings, conclusions and any recommendations to [party to whom credit union wants such reports to be made].

Each case will be considered individually in accordance with the expert advice available, and priority will be given to minimize losses (both monetary and otherwise) to the Credit Union.

Where the report of the manager of [the department that investigates fraud] provides reasonable grounds for suspecting an employee or employees of fraud or a dishonest activity, the [name of responsible party] will decide if any actions are necessary to deal with the situation and/or prevent further loss. This may require the suspension with or without pay of the employee(s) (which will take place in accordance with XXXX Credit Union's disciplinary procedures) and/or a decision as to whether further investigation is required. If an investigation results in a recommendation to terminate an employee or remove an official, the recommendation will be forwarded for review by the department responsible for handling such matters and, if necessary, review by XXXX Credit Union's outside counsel.

Where further investigation is required the [name of responsible official] in consultation with the manager of [the department that investigates fraud] and other relevant XXXX Credit Union officials will determine the format and nature of the investigation.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know; it may be necessary to consult XXXX Credit Union's outside counsel in this regard. Any violation of this restriction could have severe consequences for XXXX Credit Union and will be treated accordingly.

The Chief Operations Officer will notify XXXX Credit Union's bond carrier at an early stage to ensure that insurance matters are dealt with promptly and properly. In certain cases, it may be necessary to involve [person who handles media relations] as he/she will be responsible for dealing with any inquiries from the press and other media on the matter. Required notifications shall also be made to the appropriate credit union regulators and law enforcement agencies as required by law.

The Audit Committee {or other committee/body} will, at an appropriate time, consider the results of the investigation and assess whether there is a weakness in XXXX Credit Union's internal control, which needs to be addressed. The Audit Committee {or other committee/body}, following consultation with the relevant divisions(s), will report on the outcome to the XXXX Credit Union Board of Directors.

ADMINISTRATION

The [position responsible] is responsible for the administration, revision, interpretation, and application of this policy except where this policy assigns that role to another individual or department. The policy will be reviewed annual and revised as needed.

VOLUNTARY ANTI-FRAUD CONTROL CERTIFICATION

(Insert date)

(Insert Credit Union Name)

Voluntary Anti-Fraud Control Certification

The Board and CEO of _____(Credit Union Name)_____ certify the following:

- The Anti-Fraud and Internal Controls white paper has been distributed to the Board and Senior Management, who have reviewed its contents.
- The credit union has reviewed its anti-fraud policies and procedures and internal controls and evaluated whether different or additional controls are required.
- The credit union has evaluated whether periodically, if an expanded scope external audit by an independent party is appropriate.
- An anonymous, toll-free fraud prevention hotline will be circulated to staff and volunteers to encourage reporting of suspicious behaviors.

(Insert signature blocks)

_____

(Insert Printed Name)

(Insert Title)

(Insert Credit Union Name)

_____

(Insert Printed Name)

(Insert Title)

(Insert Credit Union Name)

Appendix F – Examination and Audit Tracking Worksheet

EXAMPLE

EXAM AND AUDIT TRACKING SHEET

TYPE: NCUA EXAM EFF. DATED 09/30/2015 UPDATED:

Procedure	Page	Responsible Person	Results	Action Taken	Timeframe to Complete	Completed
Outstanding Checks	4	V.P. of Finance	List the finding or DOR here: Ex: As of November 18, 2015 there were four money orders and seven checks that had been outstanding more than six months…	List managements plan to address finding or DOR here: Ex: On a monthly basis the VP of Finance will review the outstanding check register to ensure…	List the deadline to complete action: Ex: June 30, 2016	
Other Real Estate Owned (OREO)	4	V.P. of Finance and V.P. of Lending	The foreclosed properties for Jones and Smith have not been transferred to OREO, even though the sheriff's sales have occurred.	Loans were moved to the OREO account on 12-15-2015 according to GAAP. As a result delinquencies are no longer over stated.	N/A	Yes

Appendix G – Whistleblower Hotline

A whistleblower hotline is an integral part of the credit union's compliance and ethics program. Research indicates that employee hotlines facilitate the detection of unethical or unlawful conduct, as tips are the most common detection method for fraud in companies with or without hotlines.

To assist Michigan Credit Unions, the Michigan Credit Union League has established a Whistleblower Hotline for credit unions, credit union officials, employees and others to report suspected fraud anonymously and confidentially. When a call is made to the hotline the staff will ask the caller if the credit union has a designated person who is to receive reports of fraud, irregular or other suspicious activity within the credit union to whom the tip can be reported for investigation. If so, MCUL staff will then report the tip to the designated individual anonymously on behalf of the caller. If no designated individual is provided the tip will be reported by MCUL staff to the Supervisory Committee Chair or Board Chair if the credit union does not have a Supervisory Committee.

Effective and expeditious response to reports of fraud will help send a message to employees, thereby instilling confidence in credit union leadership, possibly preventing the reporting of suspected wrongdoing to regulators.

The hotline should be made available to all employees.

Michigan Credit Union League
Anonymous Whistleblower Hotline
800.262.6285 ext. 193

For more information, visit mcul.org.