BROUGHT TO YOU BY:

AuditLink

Internal Controls 101

Protections Every Credit Union Should be Using

May 20, 2019

This document is presented by the auditing and compliance experts at Audit Link. It is designed to help credit union leaders review their strategies for mitigating internal fraud and describing basic internal controls and tactics credit unions can use to protect themselves from bad actors.

Contents

Introduction

These days there seems to be an embezzlement reported in the trades at least monthly. These cases are not small and, in many cases, can cost the credit union its charter.

Recently a $40 million-dollar embezzlement was uncovered at CBS Employees Credit Union in Studio City, CA. In reading the indictment it became immediately evident there was a true lack of basic internal controls being exercised by the credit union. Audit Link believes that had these controls been in place, the credit union would have caught the criminal long before dollars totaling *double the credit union's asset size* had disappeared.

Some of these controls may seem self-evident, but based on this embezzlement case and many others, it appears that many of these may simply have been forgotten by many credit unions.

Recommended Controls for: Financial Statements

Use your financial statements to shine a light on potential fraudulent activity in your credit union's books.

Goal/Strategy	Recommended Tactic(s)
Detecting a second set of books	▪ Compare the full financial statement to the financial configuration on the core and verify against the member trial balance.
Detecting hidden accounts	▪ Reconcile the trial balance against control general ledger accounts.
Detecting undetected usage of G/Ls	▪ Determine if zero balance G/Ls are suspended from printing on financials. Always print a full financial statement.
Detecting use of suspense accounts to wash activity	▪ The individual who completes reconciliations should be audited on a surprise basis, paying particular attention to suspense and settlement general ledgers.
Detecting activity being hidden from third-party auditors and examiners	▪ Review reversing general ledger entries for the prior quarter after the call report has been filed. Every big embezzlement case had this as methodology for hiding activity from examiner.

Goal/Strategy	Recommended Tactic(s)
	▪ Review of significant G/L postings made prior to the call report and then reversed afterward.
Detecting the use of control accounts to mask activity	▪ Monthly audit of all manual entries made to control accounts.

Recommended Controls for: Cash Counts

To watch for theft of cash from the vault, ATMs, TCDs, teller drawers.

Goal/Strategy	Recommended Tactic(s)
Detecting theft of cash	▪ Review of G/L postings to all cash related G/L's prior to and after the surprise cash counts. Money can and has been moved from vault to cash in transit just prior to a surprise cash count. ▪ Do not develop a routine for cash counts. A surprise is just that. ▪ Unstrap bills and always count TCDs and ATMs.

Recommended Controls for: Movement of Money

To detect anomalies on the call report.

Goal/Strategy	Recommended Tactic(s)
Historical analysis of general ledger history	▪ On occasion have specific G/L accounts reviewed for a specific period of time that spans the call report period.

Recommended Controls for: Audit and Exams

Goal/Strategy	Recommended Tactic(s)
Making sure you are paying attention to the audit	▪ Question the *de minimis* decisions with third party auditors prior to completing the annual financial audit. ▪ Interview the firm on their validation and testing methodologies prior to the engagement for investments, corporate statements, and member accounts.
Detecting manipulation of member account information	▪ Require two individuals to be involved in the generation of the AIRES file prior to supplying it to a third-party auditor or examiner. Optimally it should be done by a disinterested party.

Recommended Controls for: Uncovering Single Position Fraud

Goal/Strategy	Recommended Tactic(s)
Detecting fraud by a single employee who is the only person performing the daily duties	▪ Require 5 consecutive business days of vacation with no access to the core for those responsible for maintaining general ledger, posting items, and generating financial statements. ▪ Have someone else perform the duties of the other staff member while they are on leave.

Recommended Controls for: Money Movement Through the Check Register

Goal/Strategy	Recommended Tactic(s)
Detecting money being stolen through G/L accounts that are not frequently reconciled or reviewed	▪ Audit the check register for checks cut out of G/Ls vs. member accounts to determine if they look appropriate.

Recommended Controls for: Theft of Money through Accounts Payable

Goal/Strategy	Recommended Tactic(s)
Detecting money being stolen by creating fictitious vendors	▪ Verify that the person approving an invoice is not the one cutting the checks. ▪ Audit new account payable records to verify the existence of the vendor.

Recommended Controls for: Improper Use of Member Accounts

Goal/Strategy	Recommended Tactic(s)
Detecting the use of the base member account(s) to mask activity	▪ Audit statements monthly for suspicious activity. ▪ Credit unions should have a policy in place on exactly what should be allowed to flow through these accounts.
Detecting CU employee accounts being used to transfer money from others members or G/Ls	▪ Annually verify what accounts employees are on. ▪ Monthly review activity in accounts and be mindful of transfers from G/L entries.
Detecting transactions being masked on member account statements to cover up activity	▪ If the core allows the suppression of activity or sub accounts then audit those transactions and accounts which were set not to appear.
Detecting manipulation of member data to mask activities through file maintenance	▪ Be thoughtful when choosing individuals to do the reviews, train them to be suspicious, give them the authority to research and report. ▪ Understand those fields that could be used to cover up illegal activity. Always review changes against source documents.
Detecting money being stolen from accounts that are dormant	▪ Ask questions when reviewing higher risk activity such as transactions on dormant accounts. ▪ Review file maintenance for accounts that were reset for dormancy monitoring and had other subsequent changes such as address or email. ▪ The one who monitors dormant account activity should not have teller line authority.

Recommended Controls for: Annual Audits of Access Privileges

Goal/Strategy	Recommended Tactic(s)
Detecting areas where segregation of duty elevates the risk of fraud	▪ Auditing employee access privileges to the core platform for appropriate segregation of duty. Reviews should be done quarterly.

Other General Tips and Recommendations

- When training your staff, always interject a reminder that someone is always watching what they are doing.

- Keep an eye open for outrageous changes in life circumstances or lifestyle. These should always be questioned and verified. When it comes to lifestyle changes, this isn't the time to be politically correct.